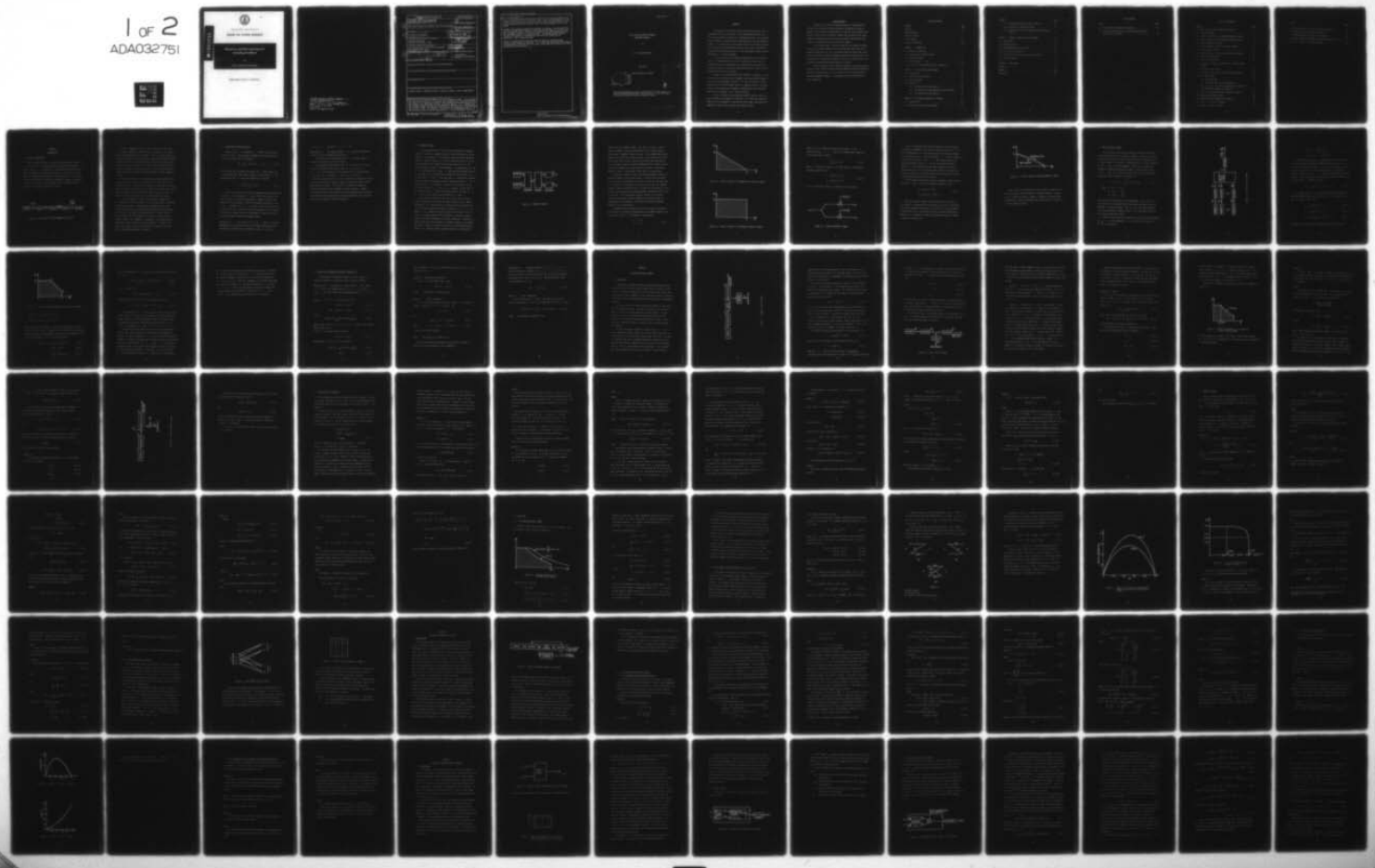
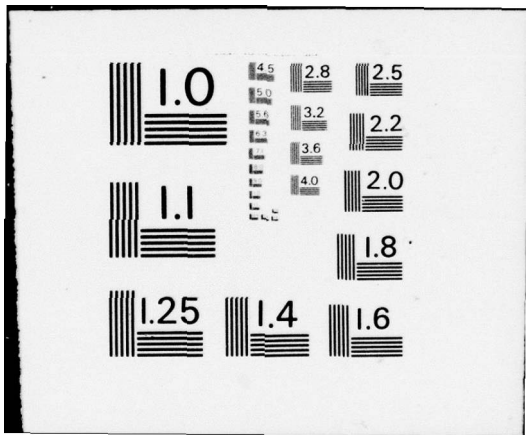
AD-A032 751 STANFORD UNIV CALIF STANFORD ELECTRONICS LABS F/G 17/2
MULTI-USER AND WIRETAP CHANNELS INCLUDING FEEDBACK.(U)
JUL 76 S K LEUNG-YAN-CHEONG F44620-73-C-0065
UNCLASSIFIED TR-6603-2 AFOSR-TR-76-1197 NL

1 OF 2
ADA032751




1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6

STANFORD UNIVERSITY

CENTER FOR SYSTEMS RESEARCH

Multi-User and Wiretap Channels Including Feedback

by

S. K. Leung-Yan-Cheong

Information Systems Laboratory

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER: AFOSR - TR - 76 - 1197
2. GOVT ACCESSION NO.
3. RECIPIENT'S CATALOG NUMBER

4. TITLE (and Subtitle): Multi-User and Wiretap Channels Including Feedback.
5. TYPE OF REPORT & PERIOD COVERED: Interim rept.
6. PERFORMING ORG. REPORT NUMBER: 6603-2

7. AUTHOR(s): S.K. Leung-Yan-Cheong
8. CONTRACT OR GRANT NUMBER(s): F44620-73-C-0065, NSF-GK-33250

9. PERFORMING ORGANIZATION NAME AND ADDRESS:
Stanford University
Stanford, California 94035

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS: 61102F 2304/A6

11. CONTROLLING OFFICE NAME AND ADDRESS:
Air Force Office of Scientific Research/NM
Bolling AFB, Bldg. 410
Washington, D.C. 20332

12. REPORT DATE: July 1976
13. NUMBER OF PAGES: 107

14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office): TR-6603-2, SU-SEL-76-027

15. SECURITY CLASS. (of this report): UNCLASSIFIED
15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

wiretap channel, information theory, broadcast channel, secure communication

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The concept of the wiretap channel was first proposed by Wyner. He considered the case in which data is to be transmitted reliably over a discrete memoryless main channel to a legitimate receiver. The wiretapper views the output of the main channel through another discrete memoryless channel. It is assumed that the wiretapper knows the code being used and his only handicap is the additional noise in his signal. The problem is to maximize the transmission rate R to the legitimate receiver and the equivocation d of the wiretapper. (cont'd.)

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED (332 400)
SECURITY CLASSIFICATION OF THIS PAGE (When Data E

20. Abstract (cont'd.)
In this dissertation, the additive white Gaussian noise wiretap channel is introduced and the set of all achievable (R,d) pairs is determined explicitly through the use of certain special properties of the Gaussian channel. Some useful characterizations of a special class of wiretap channels are also explored.

A model of the wiretap channel with feedback is proposed. It turns out that with the introduction of feedback, even when the main channel is inferior to the wiretapper's channel, it is still possible to reliably communicate with the legitimate receiver in complete secrecy. The binary erasure wiretap channel with feedback is examined and inner and outer bounds on the achievable (R,d) region are given.

Finally, a scheme for enlarging the capacity region of multiple-access channels using feedback is analyzed. It is shown that conditions under which an enlargement is possible are fairly weak, indicating that feedback can almost increase the capacity region.

SEL-76-027

MULTI-USER AND WIRETAP CHANNELS INCLUDING FEEDBACK

by

S. K. Leung-Yan-Cheong

July 1976

Technical Report No. 6603-2

This work was supported in part by the National Science Foundation (Grants GK-33250 and ENG-10173), and from the U. S. Air Force Office of Scientific Research (Contract F44620-73-C-0065).

ABSTRACT

The concept of the wiretap channel was first proposed by Wyner. He considered the case in which data is to be transmitted reliably over a discrete memoryless main channel to a legitimate receiver. The wiretapper views the output of the main channel through another discrete memoryless channel. It is assumed that the wiretapper knows the code being used and his only handicap is the additional noise in his signal. The problem is to maximize the transmission rate R to the legitimate receiver and the equivocation d of the wiretapper.

In this dissertation, the additive white Gaussian noise wiretap channel is introduced and the set of all achievable (R,d) pairs is determined explicitly through the use of certain special properties of the Gaussian channel. Some useful characterizations of a special class of wiretap channels are also explored.

A model of the wiretap channel with feedback is proposed. It turns out that with the introduction of feedback, even when the main channel is inferior to the wiretapper's channel, it is still possible to reliably communicate with the legitimate receiver in complete secrecy. The binary erasure wiretap channel with feedback is examined and inner and outer bounds on the achievable (R,d) region are given.

Finally, a scheme for enlarging the capacity region of multiple-access channels using feedback is analyzed. It is shown that conditions under which an enlargement is possible are fairly weak, indicating that feedback can almost always increase the capacity region.

ACKNOWLEDGEMENTS

I would like to express my deep gratitude to Professor Martin Hellman for his expert assistance and advice throughout my doctoral program. His accessibility and readiness to help are greatly appreciated. Special thanks are due to Professor Thomas Cover who gave me the opportunity to collaborate with him on several problems. My work with both Professors Hellman and Cover has been most enjoyable.

I also wish to thank : Professor John Gill for numerous valuable discussions; Professor Robert White for reading the thesis and for his helpful remarks; Ms. Susi Lilly and Frances Jones for typing the dissertation; the numerous student colleagues, especially Aydano Carleial, who provided such a stimulating atmosphere to work in; my parents whose love, patience and understanding made everything possible.

Financial support for my studies at Stanford came from the English Speaking Union, from the National Science Foundation (Grants GK-33250 and ENG-10173), and from the U. S. Air Force Office of Scientific Research (Contract F44620-73-C-0065). I am grateful to these institutions for their generosity.

Table of Contents

List of Tables

List of Illustrations

Figure | Page

CHAPTER 1

INTRODUCTION

1.1 GENERAL INTRODUCTION

Modern information theory is based on the work done by Shannon [1] in the late 1940's. The communication system which he analyzed is shown in figure 1.1. The information source generates random messages which are encoded into channel input signals. These signals are then sent over the communication channel to the destination. In the process of being transmitted, the signals are subjected to random disturbances, or noise. On the basis of the received signal, the decoder makes an estimate of the message output by the source.

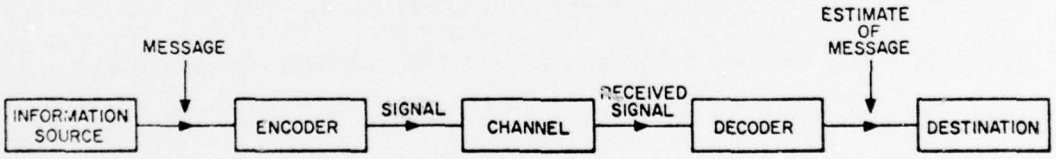


Figure 1.1 - BASIC POINT TO POINT COMMUNICATION SYSTEM

Shannon's fundamental result is that if the rate of the source is less than a quantity C, referred to as the capacity of the channel, then reliable communication is possible. That is, through appropriate coding, the decoder can estimate source messages with arbitrarily small probability of error. On the other hand, if the source rate exceeds capacity, this is not possible. This result, known as the noisy channel coding theorem, was very surprising as it had previously been believed that there was a gradual trade-off between rate and probability of error.

Since the pioneering work of Shannon, many other significant contributions have been made to the theory as testified to by the vast literature [2, 3]. During the last few years, a great deal of research effort has been devoted to the study of multi-user communication systems, that is, systems involving more than a single source and a single receiver. In this dissertation, we will analyze some such systems.

In this introductory chapter, some previously studied multi-user networks are briefly reviewed. In the second chapter, the concept of the wiretap channel is presented and the complete set of rate-equivocation pairs for the additive white Gaussian noise wiretap channel is found. Some useful characterizations of a special class of wiretap channels are also examined. In chapter 3, a model for the wiretap channel with feedback is introduced. An innerbound and an outerbound to the achievable region are derived. A scheme for enlarging the capacity region of multiple-access channels using feedback is proposed and analyzed in chapter 4.

1.2 PRELIMINARIES AND DEFINITIONS

Suppose $\{U_i\}_{i=1}^{L}$ is a sequence of L letters from a discrete stationary source. Then the rate or entropy of the source measured in bits per source letter is defined as

$$H(U) = \lim_{L \to \infty} \frac{1}{L} H(U_1, U_2, \ldots, U_L). \qquad (1.2.1)$$

Let us assume that an encoder takes blocks of L source letters at a time and maps them into channel codewords of block length N. The communication rate R in bits per channel use is given by

$$R = \frac{H(U_1, U_2, \ldots, U_L)}{N} . \qquad (1.2.2)$$

In the single source, single receiver communication system depicted in figure 1.1, a single number C is sufficient to describe the network's capacity for reliable communication. However, in multi-user networks we are interested in several simultaneous transmission rates $R_1, R_2, \ldots, R_M$ where R_i, $1 \leq i \leq M$ refers to the rate over the ith communication link. These rates are often considered as a rate vector $\underline{R}$ and lead to a generalization of the concept of capacity to that of a capacity boundary surface in Euclidean M-space.

Definition 1.1: A rate vector $\underline{R} = (R_1, R_2, \ldots, R_M)$ is said to be achievable by a communication network if reliable transmissions are simultaneously possible over the network at rates $\underline{R} - \underline{\varepsilon}$ for all

$\underline{\varepsilon} = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_M)$ where $\varepsilon_i > 0$, $1 \leq i \leq M$.

Definition 1.2: The capacity region $\mathcal{C}$ of a communication network is the set of all achievable rate vectors $\underline{R}$.

It follows from the definitions that $\mathcal{C}$ is a closed subset of the positive orthant of Euclidean M-space.

A time-sharing argument shows that $\mathcal{C}$ is also convex: If $\underline{R}_1$ and $\underline{R}_2$ are two achievable rate vectors, then $\underline{R} = \alpha \underline{R}_1 + (1-\alpha) \underline{R}_2$, $0 \leq \alpha \leq 1$, is also achievable by the scheme which uses codes designed for $\underline{R}_1$ and $\underline{R}_2$ for fractions α and $(1-\alpha)$ of the time.

The next two sections will be a brief review of two extensively studied multi-user communication networks, namely the broadcast channel and the multiple-access channel. In both cases, the channels perturbed by additive white Gaussian noise (AWGN) are used as examples. Schemes for achieving rates on the boundary of the corresponding capacity regions are outlined as they provide some insight and perspective into the problems to be considered in subsequent chapters.

1.3 BROADCAST CHANNEL

In an innovative paper in 1972, Cover [4] analyzed the broadcast channel in which one transmitter wishes to send information to several receivers simultaneously. For simplicity, the two-receiver broadcast channel is shown in figure 1.2. We shall assume that there is no common information to be transmitted to the two receivers (i.e., the source messages W_1 and W_2 are independent). The encoder maps W_1 and W_2 into the channel input signal $\underline{X}$. The memoryless broadcast channel is specified by a set of conditional probability distributions $P_{Y_1Y_2|X}$ on the outputs Y_1 and Y_2 given the input X. Because the receivers are not allowed to collaborate, possible dependence between Y_1 and Y_2 conditioned on X is irrelevant. Thus only a knowledge of the marginal distributions $P_{Y_1|X}$ and $P_{Y_2|X}$ is required. On the basis of his channel output $\underline{Y_1}$, the first receiver makes an estimate $\hat{W}_1$ of W_1. Similarly, the second receiver estimates W_2 from $\underline{Y_2}$.

One of the main results to come out of Cover's work is that if separate messages are to be sent to several receivers from a common transmitter, it is often possible to do better than just time-sharing the transmitter between the receivers to achieve $\underline{R} = (\alpha\, C_1, (1-\alpha)\, C_2)$ where C_i, $i=1,2$ denotes the capacity from the transmitter to the ith receiver. Roughly speaking, this improvement is achieved by superimposing high-rate information on low-rate information. Although the capacity region of general memoryless broadcast channels is not known, some special classes of channels for which it has been determined are given in [4]. Capacity regions typifying those of the incompatible

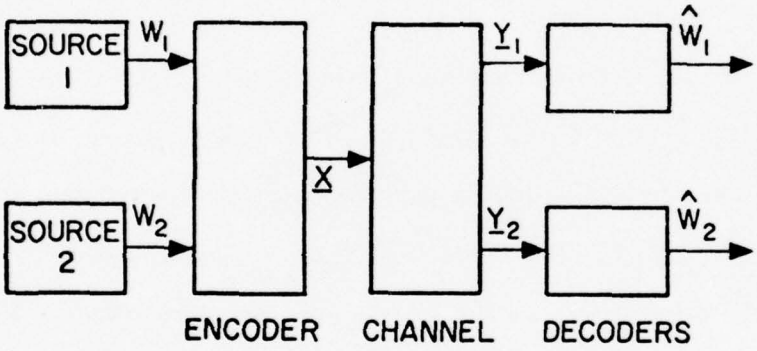


Figure 1.2 - BROADCAST CHANNEL

channel and the orthogonal channel are shown in figures 1.3 and 1.4. These two channels represent the smallest and the largest capacity regions that a broadcast channel can have. In an incompatible channel, communication with either receiver results in the transmission of pure noise to the other receiver; one can do no better than time-sharing. In an orthogonal channel, efficient communication with either receiver in no way interferes with communication to the other: each channel performs as well in the presence of the other as it would alone.

An important concept is that of the degraded broadcast channel in which the channel to the second receiver is statistically equivalent to the cascade of the channel to the first receiver and some other channel. Bergmans [5] established an achievable rate region for degraded broadcast channels through the use of a satellite coding scheme in which closely spaced codewords have distinguishable meanings only for the better receiver. The corresponding converse theorems for the binary symmetric and Gaussian broadcast channels were proved by Wyner [6] and Bergmans [9] respectively. The converse for general degraded channels is due to Gallager [7].

A degraded broadcast channel for which Cover gave an achievable rate region is the additive white Gaussian noise (AWGN) broadcast channel shown in figure 1.5. The channel is described by

$$\begin{aligned} Y_1 &= X + n_1 \\ Y_2 &= X + n_2 \end{aligned} \qquad (1.3.1)$$

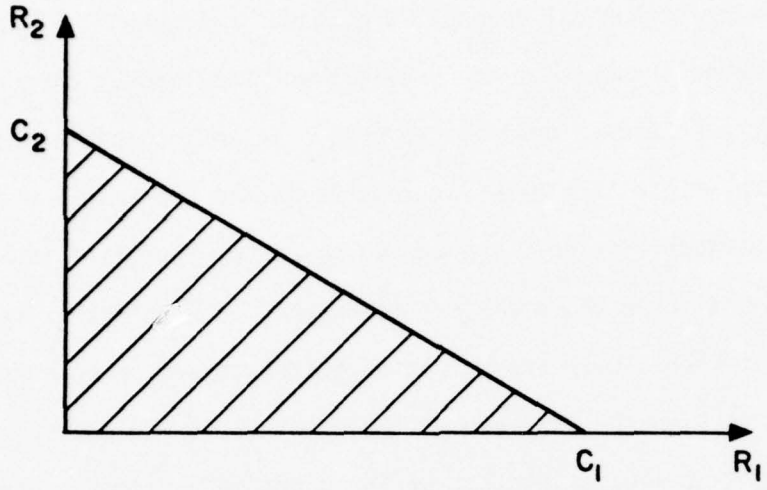


Figure 1.3 - CAPACITY REGION OF AN INCOMPATIBLE BROADCAST CHANNEL

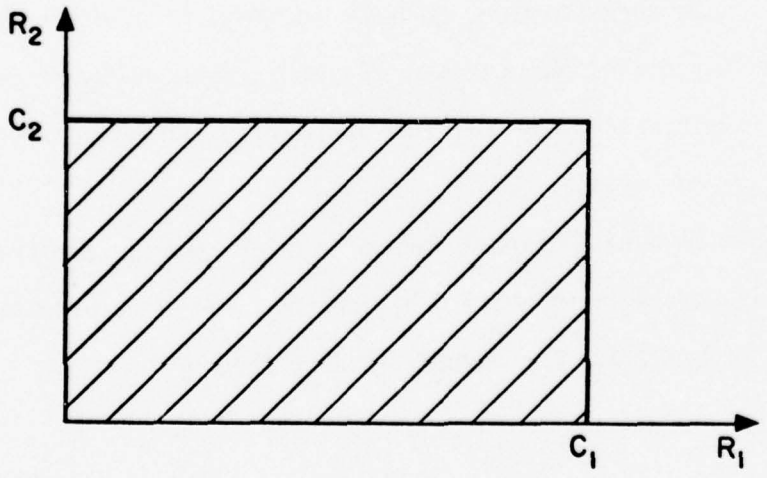


Figure 1.4 - CAPACITY REGION OF AN ORTHOGONAL BROADCAST CHANNEL

where n_1 and n_2 are Gaussian noises with variances σ_1^2 and σ_2^2 respectively and $\sigma_1^2 < \sigma_2^2$. There is an average power constraint on the input signal, given by

$$E \sum_{t=1}^{N} X_t^2 \leq NP \tag{1.3.2}$$

where N is the block length. It is well known [1, 3] that the individual capacities are

$$\begin{aligned} C_1 &= \frac{1}{2} \log \left(1 + \frac{P}{\sigma_1^2}\right) \\ C_2 &= \frac{1}{2} \log \left(1 + \frac{P}{\sigma_2^2}\right) \end{aligned} \tag{1.3.3}$$

bits per transmission, where all logarithms are to the base 2.

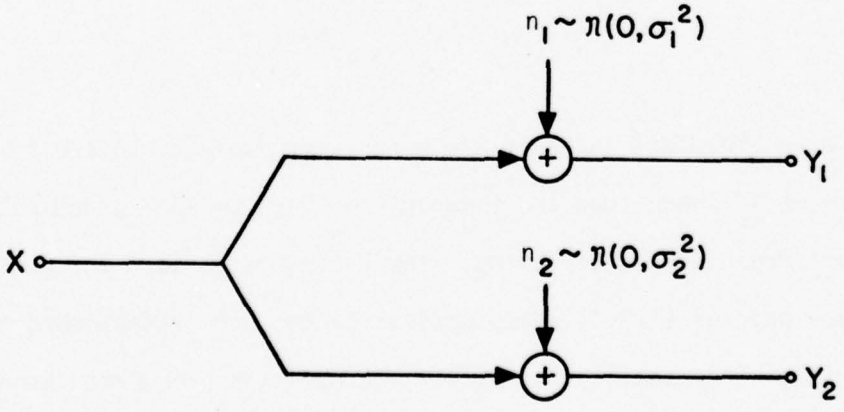


Figure 1.5 - GAUSSIAN BROADCAST CHANNEL

Cover [4] suggested the following scheme for improving upon the time-sharing performance. The idea is to devote a fraction $\bar{\alpha} = (1-\alpha)$ of the allowed power P to the transmission of the message intended for the second receiver. The remaining power αP is used to communicate with the first receiver. Since $\sigma_1 < \sigma_2$, any message which can be reliably decoded by receiver 2 can also be reliably decoded by receiver 1. By first decoding the signal intended for receiver 2 and subtracting it from his received signal, the first receiver can convert his channel to a Gaussian channel with input power constraint αP and additive Gaussian noise of variance σ_1^2.

Using the above superposition scheme, independent transmissions to receivers 1 and 2 can be simultaneously achieved at rates

$$R_1 = \frac{1}{2} \log \left(1 + \frac{\alpha P}{\sigma_1^2}\right)$$
$$R_2 = \frac{1}{2} \log \left(1 + \frac{\bar{\alpha} P}{\alpha P + \sigma_2^2}\right) . \qquad (1.3.4)$$

Gaussian broadcast channels are more extensively discussed in [8], where it is shown that the time-sharing rate region is dominated by suitable frequency multiplexing. The latter is in turn dominated by the rate pair of (1.3.4) whose optimality has been established by Bergmans [9]. The capacity region for the Gaussian broadcast channel is depicted in figure 1.6.

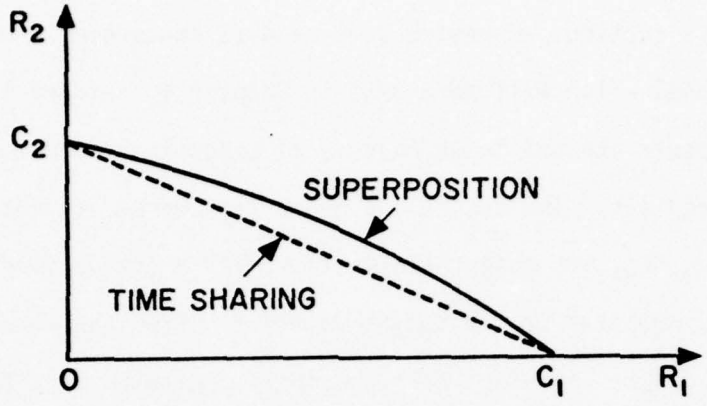


Figure 1.6 - CAPACITY REGION OF GAUSSIAN BROADCAST CHANNEL

Cover [10] and van der Meulen [11] have found an achievable rate region for general discrete memoryless broadcast channels. However, no way is known for proving a converse. Recently it has been shown by Gelfand [12] that the achievable rate region given in [10] and [11] is not the capacity region.

1.4 MULTIPLE-ACCESS CHANNEL

In this section, we review some results concerning the multiple-access channel which will be useful in Chapter 4. Figure 1.7 shows the mulitple-access channel in which several transmitters communicate with a single receiver. The channel is characterized by its input alphabets $\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_M$, its output alphabet $\mathcal{Y}$, and a set of conditional probability measures on the output signal Y given the input signals $X_1, X_2, \ldots, X_M$. For simplicity, we shall deal with only two senders and assume that the channel is memoryless, i.e.

$$P(\underline{y}|\underline{x}_1, \underline{x}_2) = \prod_{i=1}^{N} P(y_i|x_{1i}, x_{2i}) \qquad (1.4.1)$$

where $\underline{y} = (y_1, \ldots, y_N)$

$\underline{x}_1 = (x_{11}, \ldots, x_{1N})$

$\underline{x}_2 = (x_{21}, \ldots, x_{2N})$

The sources will be considered to be independent. (See [13] for an investigation of the savings that can be achieved when the sources are dependent.) Recently Ahlswede [14], Liao [15], and Slepian and Wolf [13] have determined the capacity region $\mathcal{C}$ of a two-input, single output, discrete memoryless channel:

$\mathcal{C}$ = closure of the convex hull of the union, over all input distributions $P_{X_1, X_2}(\,\cdot\,,\,\cdot\,)$ with independent X_1, X_2, of the sets of rate pairs $\underline{R} = (R_1, R_2)$ satisfying

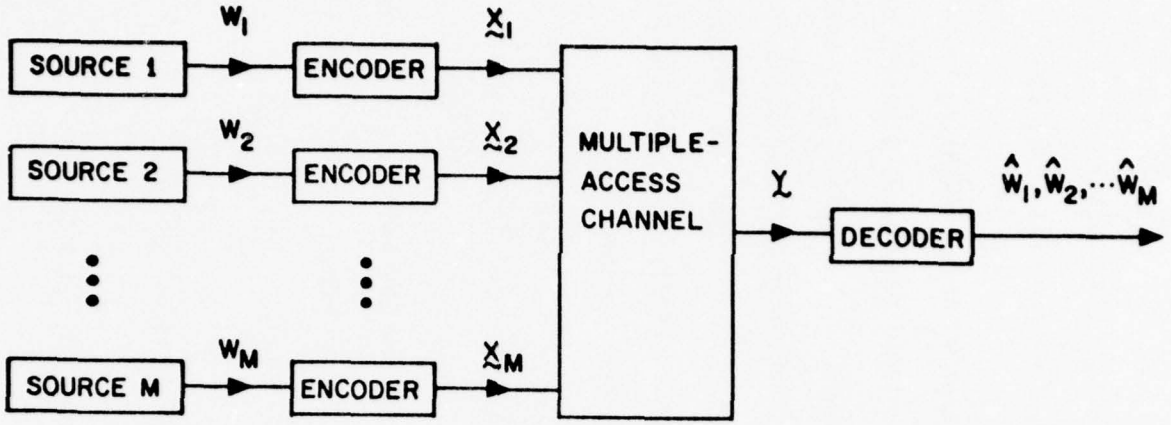


Figure 1.7 - MULTIPLE-ACCESS CHANNEL

$$
\begin{aligned}
0 \le R_1 &\le I(X_1; Y|X_2) \\
0 \le R_2 &\le I(X_2; Y|X_1) \qquad (1.4.2) \\
0 \le R_1 + R_2 &\le I(X_1, X_2; Y).
\end{aligned}
$$

The additive white Gaussian noise (AWGN) multiple-access channel is the most commonly encountered continuous alphabet channel ($\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y} = \mathbb{R}$). The output signal $Y = X_1 + X_2 + V$ where X_1 and X_2 are the input signals and V is zero-mean Gaussian noise independent of X_1 and X_2 with variance $EV^2 = \sigma^2$. There are average power constraints P_1 and P_2 on the inputs which require that the encoded messages $\underline{X}_1$ and $\underline{X}_2$ (which have N components) satisfy

$$
E \sum_{j=1}^{N} [\, X_{ij} \,]^2 \le N P_i, \quad i = 1, 2 \qquad (1.4.3)
$$

The capacity region $\mathcal{C}$ for the AWGN multiple-access channel has been determined by Wyner [16] and Cover [17]: $\mathcal{C}$ = set of all rate pairs $\underline{R} = (R_1, R_2)$ satisfying

$$
R_1 \le \frac{1}{2} \log \left(1 + \frac{P_1}{\sigma^2}\right) \triangleq C_1 \qquad (1.4.4\ a)
$$

$$
R_2 \le \frac{1}{2} \log \left(1 + \frac{P_2}{\sigma^2}\right) \triangleq C_2 \qquad (1.4.4\ b)
$$

$$
R_1 + R_2 \le \frac{1}{2} \log \left(1 + \frac{P_1 + P_2}{\sigma^2}\right) \triangleq C_{12} \qquad (1.4.4\ c)
$$

The region $\mathcal{C}$ corresponds to the shaded region shown in figure 1.8.

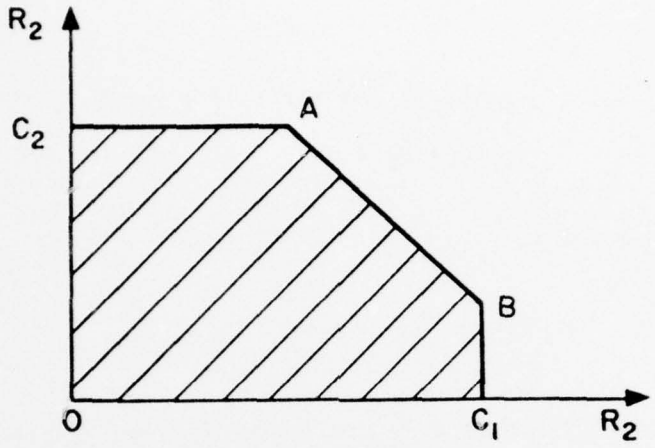


Figure 1.8 - CAPACITY REGION FOR GAUSSIAN MULTIPLE-ACCESS CHANNEL

Point A: $(C_1, \frac{1}{2} \log (1 + \frac{P_2}{P_1 + \sigma^2}))$

Point B: $(\frac{1}{2} \log (1 + \frac{P_1}{P_2 + \sigma^2}), C_2)$

The proof that points outside $\mathcal{C}$ are not achievable goes as follows: The limits on R_1 and R_2 given by (1.4.4 a) and (1.4.4 b) hold because they are the values of the channel capacities for the individual links. To verify the bound on $R_1 + R_2$, we first note that

$$I(X_1, X_2; Y) = H(Y) - H(Y|X_1, X_2) \qquad (1.4.5)$$

$$= H(Y) - H(V) \qquad (1.4.6)$$

$$= H(Y) - \frac{1}{2} \log 2\pi e\sigma^2 \qquad (1.4.7)$$

From the independence of X_1, X_2 and V, we can upperbound the variance of Y by

$$\text{var } (Y) = \text{var } (X_1) + \text{var } (X_2) + \text{var } V \qquad (1.4.8)$$

$$\leq P_1 + P_2 + \sigma^2 \qquad (1.4.9)$$

From [3, Theorem 7.4.1]

$$H(Y) \leq \frac{1}{2} \log \ 2\pi e(P_1 + P_2 + \sigma^2) \qquad (1.4.10)$$

Substitution of H(Y) in (1.4.7) yields the desired result

$$I(X_1, X_2; Y) \leq \frac{1}{2} \log (1 + \frac{P_1 + P_2}{\sigma^2}) \triangleq C_{12} \qquad (1.4.11)$$

The achievability of $\mathcal{C}$ can be proved by showing that the extreme points A and B in figure 1.8 are achievable since time-sharing then yields any point on the line connecting A and B. The whole region $\mathcal{C}$ is obtained by noting that information can be thrown away, i.e. if (R_1, R_2) is achievable, so is $(R_1 - \varepsilon_1, R_2 - \varepsilon_2)$ for $\varepsilon_1, \varepsilon_2 \geq 0$.

The following coding scheme attains a rate pair corresponding to point A, and a similar system will achieve rates corresponding to point B. For use at transmitter i, i = 1,2, we choose 2^{NR_i} independent codewords at random in the usual way according to a Gaussian distribution with mean 0 and variance $P_i' = P_i - \eta$ where $\eta > 0$ can be chosen arbitrarily small. The receiver first attempts to decode the message W_2 from the second transmitter. In so doing, it treats the signal $\underline{X}_1$ as Gaussian noise of variance P_1'. Because of the independence

of X_1 and V, the effective noise observed by the receiver in decoding W_2 is Gaussian noise of variance $(P_1' + \sigma^2)$. From the coding theorem for Gaussian channels, we know that W_2 can be reliably decoded if $R_2 < \frac{1}{2} \log (1 + \frac{P_2}{P_1 + \sigma^2})$. Once W_2 (and hence $\underline{X}_2$) has been determined, the receiver can subtract $\underline{X}_2$ from the received vector $\underline{Y}$ to obtain $\underline{Y} - \underline{X}_2 = \underline{X}_1 + \underline{V}$. But for this situation, we know that reliable transmission from the first transmitter is possible if $R_1 < C_1 = \frac{1}{2} \log (1 + \frac{P_1}{\sigma^2})$. This completes the proof that point A is achievable.

1.5 SOME USEFUL INFORMATION THEORETIC INEQUALITIES

To conclude this introductory chapter, we recall several inequalities which will be extensively used in the next chapter.

Definition 1.3: The sequence of random variables $\{X_i\}_{i=1}^{n}$ where $n \geq 3$ is said to be a Markov chain if $(X_1, X_2, \ldots, X_{j-1})$ and $(X_{j+1}, \ldots, X_n)$ are conditionally independent given X_j, $2 \leq j \leq n-1$.

Lemma 1.1 If X, Y, Z is a Markov chain, then

$$H(Z|X, Y) = H(Z|Y) \qquad (1.5.1\ a)$$

and

$$H(X|Y, Z) = H(X|Y) \qquad (1.5.1\ b)$$

Proof:

$$H(Z|X,Y) \triangleq \sum_{x,y,z} p(x,y,z) \log \frac{1}{p(z|x,y)} \qquad (1.5.2)$$

where the sum is over all $x \in \mathcal{X}$, $y \in \mathcal{Y}$, $z \in \mathcal{Z}$. Recall script letters denote sample spaces.

Since X, Y, Z is a Markov chain, we have

$$p(z|x, y) = p(z|y) \qquad (1.5.3)$$

Substituting (1.5.3) in (1.5.2), we obtain

$$H(Z|X, Y) = \sum_{y,z} p(y,z) \log \frac{1}{p(z|y)} \qquad (1.5.4)$$

$$= H(Z|Y) \qquad (1.5.5)$$

This establishes (1.5.1 a). A similar proof using $p(x|y, z) = p(x|y)$ yields (1.5.1 b).

Lemma 1.2 (Data Processing Theorem)

Let X, Y, Z form a Markov chain. Then

$$I(X; Z) \leq I(X; Y) \tag{1.5.6}$$

Proof: See Gallager [3, theorem 4.3.3].

Lemma 1.3 (Fano's Inequality)

Let U, V be random variables which take values in $\mathcal{U}$, where the number of elements, M, in $\mathcal{U}$ is finite. Let

$$\lambda = \Pr\{U \neq V\}. \tag{1.5.7}$$

Then

$$H(U|V) \leq h(\lambda) + \lambda \log (M-1) \tag{1.5.8}$$

where

$$h(\lambda) = -\lambda \log \lambda - (1-\lambda) \log (1-\lambda) \tag{1.5.9}$$

is the binary entropy function.

Proof: See Gallager [3, theorem 4.3.1].

We shall also need the following version of Fano's inequality which deals with the average bit error probability.

Definition 1.4: Suppose a sequence $\underline{v}^L = (v_1, v_2, \ldots, v_L)$ is used to approximate a sequence $\underline{u}^L = (u_1, u_2, \ldots, u_L)$. If $u_\ell \neq v_\ell$, then we say that an error has occurred in the ℓth digit and we denote the probability of such an error by $P_{e,\ell}$. We define the per symbol error probability $\langle P_e \rangle$ by

$$\langle P_e \rangle = \frac{1}{L} \sum_{\ell=1}^{L} P_{e,\ell} \tag{1.5.10}$$

Lemma 1.4 (Fano's Inequality)

Let the coordinates of $\underline{U}^L$ and $\underline{V}^L$ take values in the set $\mathcal{U}$ which has cardinality M. Let $\langle P_e \rangle$ be defined as in (1.5.10). Then

$$\frac{1}{L} H(\underline{U}^L | \underline{V}^L) \leq h(\langle P_e \rangle) + \langle P_e \rangle \log (M-1) \tag{1.5.11}$$

Proof: See Gallager [3, theorem 4.3.2]

CHAPTER 2

THE GAUSSIAN WIRETAP CHANNEL

2.1 INTRODUCTION

Traditionally, information theory has mainly been concerned with the maximum rates at which reliable communication is possible. Aside from an early paper by Shannon [18], privacy and security problems had been given very little attention in the information theoretic literature. Until recently these problems were considered mainly from a cryptographic viewpoint.

In a recent paper [19], Wyner formulated a problem in which privacy is to be taken into account. We begin this chapter with a review of Wyner's results for discrete memoryless wiretap channels. We then extend his results to the Gaussian wiretap channel and explicitly determine the complete achievable rate-equivocation region. Finally some useful characterizations of a special class of wiretap channels are examined.

The model which Wyner proposed is shown in figure 2.1. It is a form of degraded broadcast channel [5], with the novel change that one information rate is to be maximized and the other minimized. The object is to maximize the rate of reliable communication from the source to the legitimate receiver, subject to the constraint that the wiretapper learns as little as possible about the source output. The wiretapper knows the encoding scheme used at the transmitter and the decoding

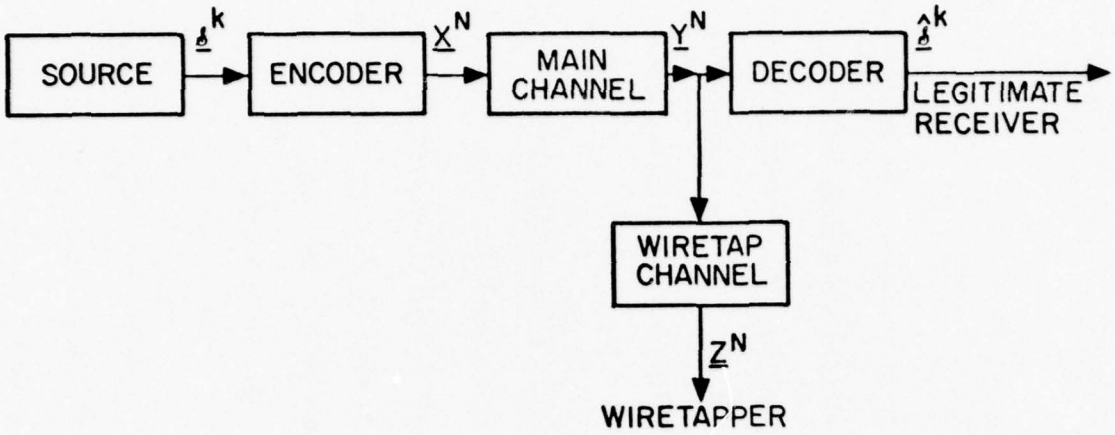


Figure 2.1 - GENERAL WIRETAP CHANNEL

scheme used at the legitimate receiver, and is kept ignorant solely by the greater noise present in his received signal. Thus, while the objective is the same as in cryptography, the technique used to achieve privacy is very different.

The source is stationary and ergodic, and has a finite alphabet. The first k source outputs $\underline{s}^k$ are encoded into an N-vector $\underline{x}^N$ which is the input to the main channel. The legitimate receiver makes an estimate $\hat{\underline{s}}^k$ of $\underline{s}^k$ based on $\underline{y}^N$, the output of the main channel, incurring a block error rate

$$P_e = \Pr \{ \underline{s}^k \neq \hat{\underline{s}}^k \}. \qquad (2.1.1)$$

$\underline{y}^N$ is also the input to the wiretap channel and the wiretapper has average residual uncertainty $H(\underline{s}^k|\underline{Z}^N)$ after observing the output, $\underline{z}^N$ of the wiretap channel. Of course, the problem remains unchanged if $\underline{z}^N$ is the output of a single channel with input $\underline{x}^N$ and statistically equivalent to the cascade of the main and wiretap channels, since dependencies between $\underline{y}^N$ and $\underline{z}^N$ are immaterial. This is not necessarily the case if feedback is allowed (see Chapter 3).

We define the fractional equivocation of the wiretapper to be

$$\Delta = H(\underline{s}^k|\underline{Z}^N) \; / \; H(\underline{s}^k) \; , \qquad (2.1.2)$$

and the rate of transmission to the legitimate receiver to be

$$R = H(\underline{s}^k) \; / \; N \; . \qquad (2.1.3)$$

Note that $\Delta = 1$ implies that the wiretapper's a posteriori uncertainty about the source output is equal to his a priori uncertainty.

Thus when $\Delta = 1$, the wiretapper is no better informed after he receives his data than he was before. We shall say that the pair (R^*, d^*) is achievable if for all $\varepsilon > 0$, there exists an encoder-decoder pair such that

$$R \geq R^* - \varepsilon \qquad (2.1.4\ a)$$

$$\Delta \geq d^* - \varepsilon \qquad (2.1.4\ b)$$

$$P_e \leq \varepsilon \qquad (2.1.4\ c)$$

Our definitions are slightly different from Wyner's original definitions. For example, Wyner defines $\Delta = H(\underline{S}|\underline{Z}) / k$. (We will drop superscripts when context permits). The new definitions are used because they allow somewhat simpler theorem statements and proofs.

The main objective is to characterize the set of achievable (R, d) pairs. In order to develop some intuition for this problem, consider the simple example depicted in figure 2.2.

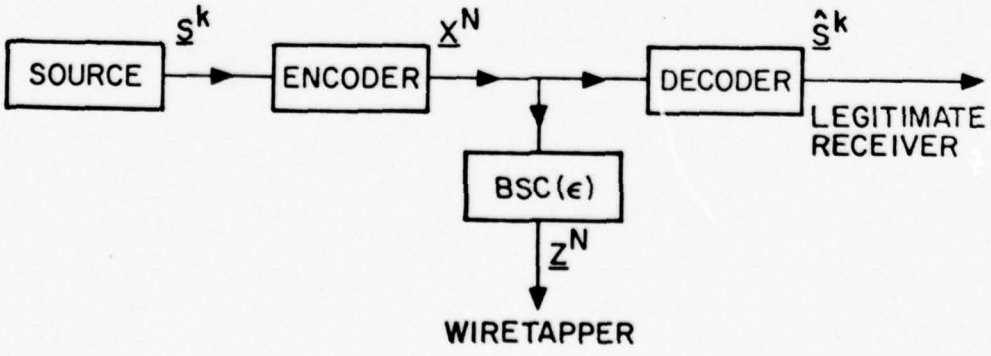


Figure 2.2 - SIMPLE WIRETAP CHANNEL

Here the source is binary symmetric, that is, successive source outputs are independent and equiprobable. The main and wiretap channels are binary symmetric channels (BSC) with crossover probabilities of 0 and ε respectively. We now analyze two very simple schemes [19] which might be used.

Scheme 1: Let $k = N = 1$ and $X = S$. Then the transmission rate R is 1 and since the main channel is noiseless, $P_e = 0$. The equivocation at the wiretapper is $\Delta = H(X|Z) = h(\varepsilon)$ where $h(\cdot)$ is the binary entropy function. Thus, this scheme achieves $(R, d) = (1, h(\varepsilon))$.

Scheme 2: Here we let $k = 1$ and N be arbitrary. Thus we are sending one of two messages in N channel uses. We partition binary N-space into two subsets: C_0 consisting of all N-vectors with an even number of 1's and C_1 consisting of all N-vectors with an odd number of 1's. If the source message is 0, the encoder outputs a vector chosen totally at random from C_0. Otherwise, the encoder output is a randomly chosen vector from C_1. Because the main channel is noiseless, the legitimate receiver can recover the source message from $\underline{X}^N$ perfectly so that $P_e = 0$. It can be shown that $H(S|\underline{Z}^N) = h\left(\frac{1}{2} - \frac{1}{2}(1 - 2\varepsilon)^N\right)$ which tends to 1 as $N \to \infty$. This means that as $N \to \infty$, the wiretapper becomes totally confused. However, as $N \to \infty$ the transmission rate $R = \frac{1}{N} \to 0$. Thus the question arises as to whether it is possible to transmit reliably at a positive rate and yet at the same time completely foil the wiretapper.

Wyner has determined the complete achievable (R, d) region when both channels are discrete memoryless channels. He shows that in most cases there is a secrecy capacity $C_s > 0$ such that $(R, d) = (C_s, 1)$ is achievable. Thus, it is possible to reliably transmit information to the legitimate receiver up to a rate C_s in essentially perfect secrecy. More generally, we have

Theorem 2.1 (Wyner).

Let $p_X(\cdot)$ be a probability distribution on the input of the main channel. Define $\rho(R)$, $R \geq 0$ to be the set of p_X such that $I(X; Y) \geq R$. For $0 \leq R \leq C_M$, where C_M is the capacity of the main channel, let

$$\Gamma(R) = \max_{p_X \in \rho(R)} I(X; Y|Z) \qquad (2.1.5)$$

Then the set of all achievable (R, d) pairs is given by

$$\mathcal{R}^* = \{(R, d) \mid 0 \leq R \leq C_M, 0 \leq d \leq 1, R\, d \leq \Gamma(R)\} \qquad (2.1.6)$$

if both channels are discrete and memoryless.

For the example of figure 2.2, application of theorem 2.1 shows that the set of achievable points is defined by

$$R \leq 1 \qquad (2.1.6\ a)$$

$$d \leq 1 \qquad (2.1.6\ b)$$

$$R\, d \leq h(\varepsilon) \qquad (2.1.6\ c)$$

For more details, see Appendix I. This result implies that scheme 1 which achieves $R = 1$, $d = h(\varepsilon)$ is optimal in that for $R = 1$, the maximum achievable equivocation is $h(\varepsilon)$. On the other hand, scheme 2 which achieves $R = 0$, $d = 1$ is not optimal since in fact for $d = 1$, it is possible to transmit up to a rate $R = h(\varepsilon)$.

The family of achievable (R, d) points in (2.1.6) is sketched in figure 2.3.

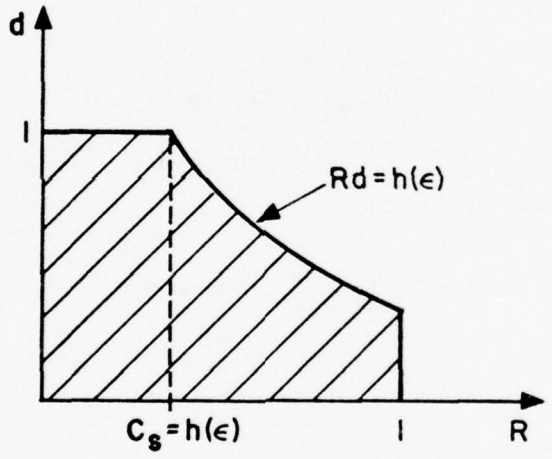


Figure 2.3 - COMPLETE ACHIEVABLE (R, d) REGION FOR A SIMPLE WIRETAP CHANNEL

As noted by Wyner, this region is not convex. Surprisingly, however, $Rd = c$ as in (2.1.6 c) corresponds to a time sharing curve as established in the following lemma.

Lemma 2.1

Let $R_1 d_1 = R_2 d_2 = c$, a constant. Assume $R_1 > R_2$ and hence $d_1 < d_2$. If the points (R_1,d_1) and (R_2,d_2) are achievable then through time-sharing any point (R,d) with $R_2 \leq R \leq R_1$, $d_1 \leq d \leq d_2$ and $Rd = c$ is achievable.

Proof:

Consider a block of N channel uses. Assume that for αN transmissions we operate at (R_1,d_1) and for $(1-\alpha)N$ transmissions we operate at (R_2,d_2). Then the effective equivocation is

$$d = \frac{\alpha N R_1 d_1 + (1-\alpha) N R_2 d_2}{\alpha N R_1 + (1-\alpha) N R_2} \quad . \tag{2.1.7}$$

The effective transmission rate is

$$R = [\alpha N R_1 + (1-\alpha) N R_2]/N \tag{2.1.8}$$

so that

$$Rd = \alpha R_1 d_1 + (1-\alpha) R_2 d_2. \tag{2.1.9}$$

We see that time sharing averages the product $R_i d_i$ and if $R_1 d_1 = R_2 d_2 = c$ then $Rd = c$. □

This lemma will be of importance in establishing the achievable (R,d) region for the Gaussian wire-tap channel, shown in figure 2.4. As before, the source is a stationary, ergodic, finite alphabet source. The noise vectors $\underline{n}_1^N$, and $\underline{n}_2^N$ are independent and have components which are independent identically distributed (i.i.d.) $\mathcal{N}(0, \sigma_1^2)$ and

$\mathcal{N}(0, \sigma_2^2)$, i.e. normal random variables with mean zero and variances σ_1^2 and σ_2^2 respectively. The channel is power limited in that

$$(1/N) \sum_{i=1}^{N} E(X_i^2) \leq P. \tag{2.1.10}$$

In the following two sections we utilize Wyner's framework to completely characterize the achievable (R,d) region for this Gaussian wire-tap channel. Letting

$$C_M = 1/2 \log (1 + P/\sigma_1^2) \tag{2.1.11}$$

and

$$C_{MW} = 1/2 \log (1 + P/(\sigma_1^2 + \sigma_2^2)) \tag{2.1.12}$$

denote the capacities of the main and overall wire-tap channels respectively, we shall show that the secrecy capacity is given by

$$C_S = C_M - C_{MW} \tag{2.1.13}$$

and in general, we have the following result.

Theorem 2.2

For the Gaussian wiretap channel the set $\mathcal{R}$ of all achievable (R,d) pairs is defined by

$$R \leq C_M \tag{2.1.14}$$

$$d \leq 1 \tag{2.1.15}$$

$$Rd \leq C_S. \tag{2.1.16}$$

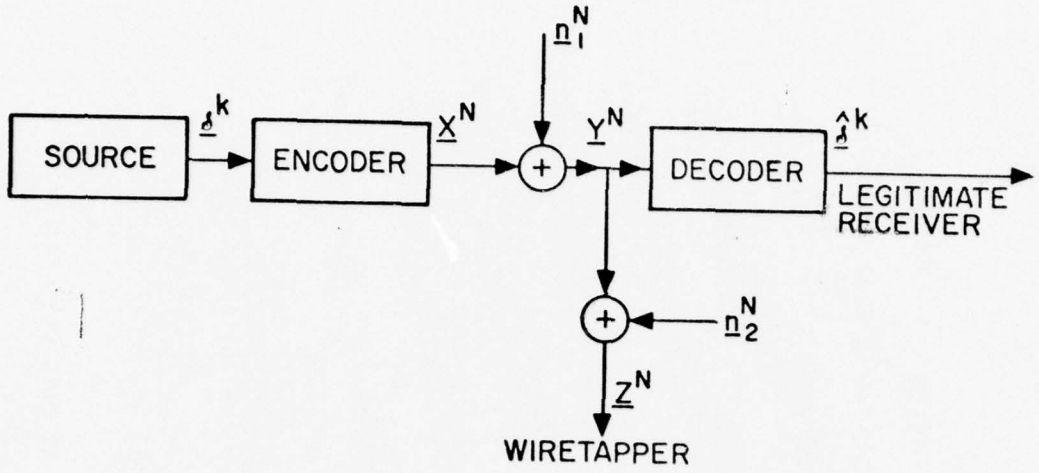


Figure 2.4 - GAUSSIAN WIRETAP CHANNEL

In the next section we establish the achievability of this region by showing that the extreme points of $\mathcal{R}$

$$(R_1, d_1) = (C_M, C_s/C_M) \tag{2.1.17}$$

and

$$(R_2, d_2) = (C_s, 1) \tag{2.1.18}$$

are both achievable. We then invoke the time sharing argument, and say that since $R_1 d_1 = R_2 d_2 = C_s$ the entire region $\mathcal{R}$ defined in theorem 2.2 is achievable.

In section 2.3 we establish the converse, that any point outside $\mathcal{R}$ is not achievable.

2.2 DIRECT HALF OF THEOREM 2.2

As noted above we need only establish that the two points (R_1,d_1) and (R_2,d_2) defined by (2.1.17) and (2.1.18) are achievable, since time sharing then implies the achievability of the entire region $\mathcal{R}$ of theorem 2.2.

The point (R_1,d_1) is trivially achieved by coding as if the wire tapper were absent. Using usual source and channel coding arguments it is possible for R to be arbitrarily close to $C_M = R_1$ and P_e to be arbitrarily close to 0. But the information gained by the wiretapper is limited by the capacity of his channel so that

$$\begin{aligned} \Delta &= H(\underline{\mathcal{A}}^k|\underline{Z}^N)/H(\underline{\mathcal{A}}^k) \\ &\geq (H(\underline{\mathcal{A}}^k) - NC_{MW})/H(\underline{\mathcal{A}}^k) \\ &= 1 - (C_{MW}/R) \end{aligned} \tag{2.2.1}$$

and as R approaches C_M, this lower bound on Δ approaches $C_s/C_M = d_1$. Thus the point (R_1,d_1) is achievable.

We will establish the achievability of $(R_2,d_2) = (C_s,1)$ by proving a somewhat stronger result, similar to that of Hellman and Carleial [20]. If $C_s = C_M/2$ theorem 2.2 states that by cutting our rate in half we can completely foil the wire tapper. Instead, we will show that it is possible to reliably send two independent messages, each at a rate near $C_s = C_M/2$, and each totally protected from the wire tapper on an individual basis. The penalty is that if the wire tapper learns one message through other means he can then also determine

the other message. In general, if $C_s \geq C_M/n$ we will show that n independent messages can be simultaneously and reliably communicated to the legitimate receiver, each at a rate near C_M/n, and each totally protected on an individual basis. However if the wire tapper learns any one message he may be able to determine all of the others. By using random noise for all but the first message we can obtain the direct half of theorem 2.2 as a special case of theorem 2.3.

Theorem 2.3

Let $\underline{u}^m$ be a sequence of m outputs from a finite alphabet, stationary, ergodic source with per letter entropy $H(\mathcal{U})$, and let $\underline{s}^p$ be any p consecutive components of $\underline{u}^m$. Then provided

$$R_t \equiv H(\underline{\mathcal{U}}^m)/N < C_M \tag{2.2.2}$$

$$R_s \equiv H(\underline{\mathcal{S}}^p)/N < C_s \tag{2.2.3}$$

it is possible by choosing N large enough, to reliably communicate $\underline{u}^m$ to the legitimate receiver in N channel uses and yet to ensure that

$$\Delta_s \equiv H(\underline{\mathcal{S}}^p|\underline{Z}^N)/H(\underline{\mathcal{S}}^p) \tag{2.2.4}$$

is arbitrarily close to 1.

Further if $\{\underline{s}^p{}_i\}_{i=1}^K$ are K such consecutive p-tuples of $\underline{u}^m$ it is possible to ensure that

$$\Delta_{si} \equiv H(\underline{\mathcal{S}}^p{}_i|\underline{Z}^N)/H(\underline{\mathcal{S}}^p{}_i) \tag{2.2.5}$$

is arbitrarily close to 1 for $1 \leq i \leq K$, with K fixed as $N \to \infty$.

Remarks:

1. An alternative notation would be to use $\underline{s}^m$ in place of $\underline{u}^m$, but then superscripts would be necessary to distinguish between the entire ergodic source output and its projection, $\underline{s}^p$, to be kept secret. This remark will hopefully remove any confusion caused by our choice of notation.

2. Until now, the entire sequence $\underline{u}^m$ was to be protected so that m equalled p, R_s equalled R_t, and Δ_s equalled Δ_t. Now the distinction between $\underline{u}^m$ and its projection $\underline{s}^p$ requires us to distinguish between the total rate R_t, and the secrecy rate R_s.

3. For memoryless sources the p outputs in $\underline{s}^p$ need not be consecutive, and more general p - dimensional projections are possible. See [20] for a generalization to linear projections.

Theorem 2.3 will be established by proving a sequence of lemmas. First, since the source is ergodic we have:

Lemma 2.2

It is possible to reliably source code $\underline{u}^m$ into a binary n-vector $\underline{u}^n$ such that each of the $\underline{s}^p_i$ are reliably determined (i.e. as $N \to \infty$ the probability of error tends to 0) by k consecutive components $\underline{s}^k_i$ of $\underline{u}^n$ and

$$n = N(C_M - 2\varepsilon) \tag{2.2.6}$$

$$k = N(C_s - \varepsilon). \tag{2.2.7}$$

with $\varepsilon > 0$.

Remark:

Script $\underline{u}^m$ denotes the entire, ergodic source output, and script $\underline{s}^p$ denotes a p-dimensional projection thereof; $\underline{u}^n$ denotes the binary source coded version of $\underline{u}^m$ and $\underline{s}^k$ denotes a k-dimensional projection thereof. Further $\underline{s}^k$ is a binary, source coded version of $\underline{s}^p$.

Proof: From (2.2.2) and (2.2.3), we can define

$$\varepsilon = \min \{(C_M - R_t)/3, (C_s - R_s)/2\} > 0 \qquad (2.2.8\ a)$$

In proving that R_s and R_t can be made to approach C_s and C_M while Δ_s is kept arbitrarily close to 1, we can redefine R_s and R_t so that

$$(C_M - R_t)/3 = (C_s - R_s)/2 = \varepsilon \qquad (2.2.8\ b)$$

where ε is given by (2.2.8 a), since excess rate can be discarded.

The noiseless source coding theorem for ergodic sources [3, theorem 3.5.3] then implies that (2.2.6) and (2.2.7) can be satisfied. There is a minor problem in ensuring that $\underline{s}^k$ consists of k consecutive bits of $\underline{u}^n$, but this is easily overcome.

If the $\{\underline{s}^p_i\}$ are disjoint we can clearly code in sub-blocks while satisfying (2.2.7) and the condition on $\underline{s}_i$ being consecutive bits of $\underline{u}$. Even if the $\{\underline{s}^p_i\}$ are not disjoint we can still satisfy these conditions. For example if $\underline{s}^p_1$ constitutes the first 3/4 of $\underline{u}^m$ and $\underline{s}^p_2$ constitutes the last 3/4 of $\underline{u}^m$ we can code $\underline{u}^m$ in four

equal sub-blocks to obtain $\underline{u}^n$. The union bound guarantees that the overall coding from $\underline{\mu}$ to $\underline{u}$ is reliable since each of the four sub-codings is reliable. □

We will henceforth deal with only one of the $\underline{s}_i$ (or $\underline{\delta}_i$) which we shall denote as $\underline{s}$ (or $\underline{\delta}$). We shall show that, over a suitable ensemble of codes, $\underline{u}$ can be reliably communicated to the receiver and Δ_s kept arbitrarily near 1, with probability which approaches 1 as $N \to \infty$. Use of the union bound then allows us to state that with probability approaching 1, all K Δ_{si} can be kept near 1. Now define an ensemble of channel codes as follows. Each code in the ensemble has 2^n codewords with blocklength N,

$$C = \{\underline{X}^1, \underline{X}^2, \ldots, \underline{X}^{2^n}\}. \qquad (2.2.9)$$

Each component of each codeword is an i.i.d. random variable with a $\mathcal{N}(0, P-\eta)$ distribution, where $\eta > 0$ is chosen so that

$$C_M(\eta) \equiv 1/2 \log (1 + (P-\eta)/\sigma_1^2) > C_M - \varepsilon \qquad (2.2.10\ a)$$

and

$$C_{MW}(\eta) \equiv 1/2 \log (1 + (P-\eta)/(\sigma_1^2 + \sigma_2^2)) > C_{MW} - \varepsilon. \qquad (2.2.10\ b)$$

Since $n = N(C_M - 2\varepsilon)$, the normal coding theorem for Gaussian channels [3, theorem 7.4.2] states that $\underline{u}^n$ is reliably transmitted to the receiver by almost all codes in the ensemble as $N \to \infty$. And as $N \to \infty$ almost all codes in the ensemble satisfy the power constraint (2.1.10) so that almost all codes satisfy both conditions as $N \to \infty$.

All that remains is to show that $\Delta_s \doteq 1$ for almost all codes in the ensemble.

Lemma 2.3

$$\Delta_s \geq [H(\underline{U}) - H(\underline{U}|\underline{S},\underline{Z}) - I(\underline{U};\underline{Z})]/NC_s \tag{2.2.11}$$

Proof: Since $\underline{s}$ is a deterministic function of $\underline{\delta}$

$$\Delta_s = H(\underline{\delta}|\underline{Z})/H(\underline{\delta}) \tag{2.2.12}$$

$$\geq H(\underline{S}|\underline{Z})/H(\underline{\delta}) \tag{2.2.13}$$

and using (2.2.3)

$$H(\underline{\delta}) \leq NC_s. \tag{2.2.14}$$

We complete the proof by showing that

$$H(\underline{S}|\underline{Z}) = H(\underline{U}) - H(\underline{U}|\underline{S},\underline{Z}) - I(\underline{U};\underline{Z}). \tag{2.2.15}$$

By definition

$$H(\underline{U}|\underline{Z}) = H(\underline{U}) - I(\underline{U};\underline{Z}) \tag{2.2.16}$$

and since $\underline{s}$ is a function of $\underline{u}$

$$H(\underline{U}|\underline{Z}) = H(\underline{U},\underline{S}|\underline{Z}) = H(\underline{S}|\underline{Z}) + H(\underline{U}|\underline{S},\underline{Z}). \tag{2.2.17}$$

□

We now proceed to bound the three terms in (2.2.11).

Lemma 2.4

There exists a sequence of source codes of increasing blocklength such that

$$H(\underline{U}) \geq NC_M\,(1-\varepsilon'-\delta) \tag{2.2.18}$$

where ε' stands for any term which tends to 0 as $\varepsilon \to 0$, and δ stands for any term which tends to 0 as $N \to \infty$ with $\varepsilon > 0$ fixed.

Proof:

From (2.2.2) and (2.2.8)

$$\begin{aligned} H(\underline{u}) &= NR_t \\ &= N(C_M - 3\varepsilon) \\ &= NC_M(1 - \varepsilon'). \end{aligned} \tag{2.2.19}$$

Since $\underline{u}$ is a deterministic function of $\underline{u}$

$$H(\underline{U}) = H(\underline{u}) - H(\underline{u}\,|\underline{U}). \tag{2.2.20}$$

Using the noiseless source coding theorem for ergodic sources [3, theorem 3.5.3] and Fano's inequality (lemma 1.3)

$$H(\underline{u}\,|\underline{U}) \leq 1 + \delta N\,, \tag{2.2.21}$$

so that

$$\begin{aligned} H(\underline{U}) &\geq NC_M(1-\varepsilon') - 1 - \delta N \\ &= NC_M(1-\varepsilon'-\delta). \end{aligned} \tag{2.2.22}$$

(Note that the two δ's are not equal). □

We now bound the second term, $H(\underline{U}|\underline{S},\underline{Z})$, in (2.2.11).

Lemma 2.5

As $N \to \infty$ almost all codes in the ensemble obey

$$H(\underline{U}|\underline{S},\underline{Z}) \leq \delta N \tag{2.2.23}$$

Proof:

Since $\underline{s}$ is a k-dimensional projection of the n-vector $\underline{u}$, given $\underline{s}$, there are only $2^{n-k} = 2^{N(C_{MW}-\varepsilon)}$ $\underline{u}$'s to be decided among on the basis of $\underline{z}$. But the codewords associated with each of these $\underline{u}$'s was chosen according to the capacity achieving distribution and from (2.2.10 b) we know the error probability given $\underline{s}$ and $\underline{z}$ tends to 0 as $N \to \infty$ for almost all codes. Use of Fano's inequality completes the proof.

Finally, use of the data processing theorem (lemma 1.2) and the definition of C_{MW} yields a bound on the third term in (2.2.11).

$$I(\underline{U};\underline{Z}) \leq N\, C_{MW}. \tag{2.2.24}$$

Combining (2.2.24) and the preceding three lemmas we find that for almost all codes

$$\begin{aligned} \Delta_s &\geq [NC_M\,(1-\varepsilon'-\delta) - \delta N - NC_{MW}]/NC_s \\ &= NC_s\,(1-\varepsilon'-\delta)/NC_s \\ &= 1-\varepsilon'-\delta. \end{aligned} \tag{2.2.25}$$

Then letting $N \to \infty$ with fixed $\varepsilon > 0$ we find that

$$\lim_{N \to \infty} \Delta_s \geq 1-\varepsilon', \tag{2.2.26}$$

and

$$\lim_{\varepsilon \to 0} \lim_{N \to \infty} \Delta_s = 1 \qquad (2.2.27)$$

for almost all codes.

This completes the proof that $(R_2, d_2) = (C_s, 1)$ is achievable.

2.3 CONVERSE THEOREM

In this section we prove the converse part of theorem 2.2, that any point (R,d) outside $\mathcal{R}$ is not achievable. That $R \leq C_M$ and $d \leq 1$ is self evident from the definitions. Our real task is to show that (2.1.16) must hold

$$R\, d \leq C_s \tag{2.1.16}$$

if P_e is arbitrarily close to 0. (Note that in this section we are dealing solely with $\underline{s}$, and not at all with $\underline{u}$ of the last section. We can therefore use R in place of R_s and Δ in place of Δ_s without ambiguity.) The proof of the following theorem is therefore the goal of this section.

Theorem 2.4

Wiht R, Δ and P_e defined as in (2.1.1) - (2.1.3)

$$R\left[\Delta - \frac{k\, P_e\, \log(\nu) + h(P_e)}{H(\underline{s}^k)}\right] \leq C_s \tag{2.3.1}$$

where ν is the size of the source alphabet and C_s is defined by (2.1.13).

If instead the per digit error rate

$$\langle P_e \rangle \equiv 1/k \sum_{i=1}^{k} \Pr(s_i \neq \hat{s}_i) \tag{2.3.2}$$

is used (2.3.1) becomes

$$R\left[\Delta - \frac{k[h(\langle P_e\rangle) + \langle P_e\rangle \log(\nu-1)]}{H(\underline{\delta}^k)}\right] \leq C_s \qquad (2.3.3)$$

Thus the use of this more lenient measure of reliability would not expand the region $\mathcal{R}$.

Remark:

If the probability of error at the legitimate receiver is not required to be arbitrarily small, theorem 2.4 can still be used to provide an outerbound on the achievable (R, d) region.

The proof of this theorem will be established through a sequence of lemmas.

Lemma 2.6

$$R\left[\Delta - \frac{k\, P_e \log(\nu) + h(P_e)}{RN}\right] \leq \frac{I(\underline{X}^N;\underline{Y}^N|\underline{Z}^N)}{N} \qquad (2.3.4)$$

and

$$R\left[\Delta - \frac{k[h(\langle P_e\rangle) + \langle P_e\rangle \log(\nu-1)]}{RN}\right] \leq \frac{I(\underline{X};\underline{Y}|\underline{Z})}{N} \qquad (2.3.5)$$

Proof:

First note that through use of the data processing theorem (lemma 1.2) and Fano's inequality (lemma 1.3)

$$H(\underline{\mathcal{A}}|\underline{Z},\underline{Y}) \leq H(\underline{\mathcal{A}}|\underline{Y})$$

$$\leq H(\underline{\mathcal{A}}|\hat{\underline{\mathcal{A}}})$$

$$\leq h(P_e) + kP_e \log(\nu). \qquad (2.3.6)$$

Then from the definitions (2.1.2), (2.1.3) of R and Δ

$$RN\,\Delta = H(\underline{\mathcal{A}}|\underline{Z}).$$

Using (2.3.6)

$$RN\,\Delta \leq H(\underline{\mathcal{A}}|\underline{Z}) - H(\underline{\mathcal{A}}|\underline{Z},\underline{Y}) + h(P_e) + kP_e \log(\nu)$$

$$= I(\underline{\mathcal{A}};\underline{Y}|\underline{Z}) + h(P_e) + kP_e \log(\nu). \qquad (2.3.7)$$

Since $\underline{\mathcal{A}}$, $\underline{X}$, $\underline{Y}$, $\underline{Z}$ form a Markov chain the data processing theorem implies

$$I(\underline{\mathcal{A}};\underline{Y}|\underline{Z}) \leq I(\underline{X};\underline{Y}|\underline{Z}). \qquad (2.3.8)$$

so

$$RN\,\Delta \leq I(\underline{X};\underline{Y}|\underline{Z}) + h(P_e) + kP_e \log(\nu) \qquad (2.3.9)$$

which with minor algebra establishes (2.3.4). Equation (2.3.5) is established in exactly the same manner, except using the per digit error rate version of Fano's inequality (lemma 1.4).

Lemma 2.7

$$I(\underline{X};\underline{Y}|\underline{Z}) = \frac{N}{2} \log\left(\frac{\sigma_1^2 + \sigma_2^2}{\sigma_1^2}\right) - [H(\underline{Z}) - H(\underline{Y})] \qquad (2.3.10)$$

Proof:

While the entropy of a continuous random variable is lacking in physical significance, if we define

$$H(A) = -\int p(a) \log [p(a)]\, da \tag{2.3.11}$$

it is known that differences in entropy are still physically meaningful as mutual information (e.g., $H(A) - H(A|B) = I(A;B)$, see [21] for a full development). We may thus write

$$I(\underline{X};\underline{Y}|\underline{Z}) = H(\underline{X}|\underline{Z}) - H(\underline{X}|\underline{Y}, \underline{Z}) = H(\underline{X}|\underline{Z}) - H(\underline{X}|\underline{Y}) \tag{2.3.12}$$

since $\underline{X}$ is independent of $\underline{Z}$, conditioned on $\underline{Y}$. Using

$$H(A,B) = H(A) + H(B|A) = H(B) + H(A|B) \tag{2.3.13}$$

(2.3.12) becomes

$$\begin{aligned} I(\underline{X};\underline{Y}|\underline{Z}) &= [H(\underline{X}) + H(\underline{Z}|\underline{X}) - H(\underline{Z})] - [H(\underline{X}) + H(\underline{Y}|\underline{X}) - H(\underline{Y})] \\ &= H(\underline{Z}|\underline{X}) - H(\underline{Y}|\underline{X}) - [H(\underline{Z}) - H(\underline{Y})]. \end{aligned} \tag{2.3.14}$$

Because the channel is memoryless

$$H(\underline{Y}|\underline{X}) = \sum_{i=1}^{N} H(Y_i|X_i) = (N/2) \log (2\pi e \sigma_1^2) \tag{2.3.15}$$

where the last expression comes from integration as in (2.3.11) [3, p. 32]. Similarly

$$H(\underline{Z}|\underline{X}) = (N/2) \log [2\pi e(\sigma_1^2 + \sigma_2^2)]. \tag{2.3.16}$$

Substituting (2.3.15) and (2.3.16) into (2.3.14) yields (2.3.10). □

Lemma 2.8

Define

$$g(P) = 1/2 \log (2\pi eP), \quad P>0 \tag{2.3.17}$$

$$g^{-1}(\alpha) = (1/2\pi e)\ e^{2\alpha} \tag{2.3.18}$$

$$A(v) = g\left[\ \sigma_2{}^2 + g^{-1}(v)\ \right] - v \tag{2.3.19}$$

Then A(v) is monotonically decreasing in v.

Proof:

$$A(v) = 1/2 \log \left[\ 2\pi e(\sigma_2{}^2 + \frac{1}{2\pi e}\ e^{2v})\ \right] - v. \tag{2.3.20}$$

Differentiating (2.3.20) yields

$$\frac{dA}{dv} = \left[\ e^{2v}/(2\pi e\sigma_2{}^2 + e^{2v})\ \right] - 1 \leq 0. \tag{2.3.21}$$

Lemma 2.9

$$H(\underline{Y}) \leq Ng(P + \sigma_1{}^2) = (N/2) \log [2\pi e(P + \sigma_1{}^2)] \tag{2.3.22}$$

Proof:

From the ordinary converse to the coding theorem [3], we know that

$$I(\underline{X};\underline{Y}) = H(\underline{Y}) - H(\underline{Y}|\underline{X}) \leq NC_M \tag{2.3.23}$$

or

$$H(\underline{Y}) \leq (N/2) \log \left[(P + \sigma_1^2)/\sigma_1^2 \right] + (N/2) \log (2\pi e \sigma_1^2)$$

$$= (N/2) \log \left[2\pi e (P + \sigma_1^2) \right]. \qquad (2.3.24)$$

Lemma 2.10

If

$$H(\underline{Y}) = Nv \qquad (2.3.25)$$

then

$$H(\underline{Z}) - H(\underline{Y}) \geq NA(v) = N\, g[\sigma_2^2 + g^{-1}(v)] - Nv. \qquad (2.3.26)$$

Remark:

This lemma follows from Shannon's convolution inequality for entropy powers which states that the entropy power of the sum of two independent random processes is at least the sum of their entropy powers. Wyner and Ziv [22] have obtained an analogous result for the binary case, known as Mrs. Gerber's Lemma.

Proof:

See Shannon [1, Theorem 15], Blachman [23] and Bergmans [9].

Combining lemmas 2.8, 2.9 and 2.10 we see that

$$H(\underline{Z}) - H(\underline{Y}) \geq N\, A[g(P + \sigma_1^2)]$$

$$= N\, g\left[\sigma_2^2 + g^{-1} g(P + \sigma_1^2) \right] - Ng(P + \sigma_1^2)$$

$$= (N/2) \log \left(\frac{P + \sigma_1^2 + \sigma_2^2}{P + \sigma_1^2} \right) \qquad (2.3.27)$$

Using (2.3.27) with lemma 2.7 yields

$$I(\underline{X};\underline{Y}|\underline{Z}) \leq \frac{N}{2} \log \left(\frac{\sigma_1^2 + \sigma_2^2}{\sigma_1^2} \right) - \frac{N}{2} \log \left(\frac{P + \sigma_1^2 + \sigma_2^2}{P + \sigma_1^2} \right)$$

$$= (N/2) \log \left(\frac{\sigma_1^2 + P}{\sigma_1^2} \right) - (N/2) \log \left(\frac{\sigma_1^2 + \sigma_2^2 + P}{\sigma_1^2 + \sigma_2^2} \right)$$

$$= N(C_M - C_{MW})$$

$$= NC_S, \qquad (2.3.28)$$

which together with lemma 2.6 completes the proof of theorem 2.4.

2.4 DISCUSSION

2.4.1 THE GAUSSIAN WIRETAP CHANNEL

Figure 2.5 show a sketch of the set $\mathcal{R}$ of all achievable (R,d) pairs defined in the statement of theorem 2.2.

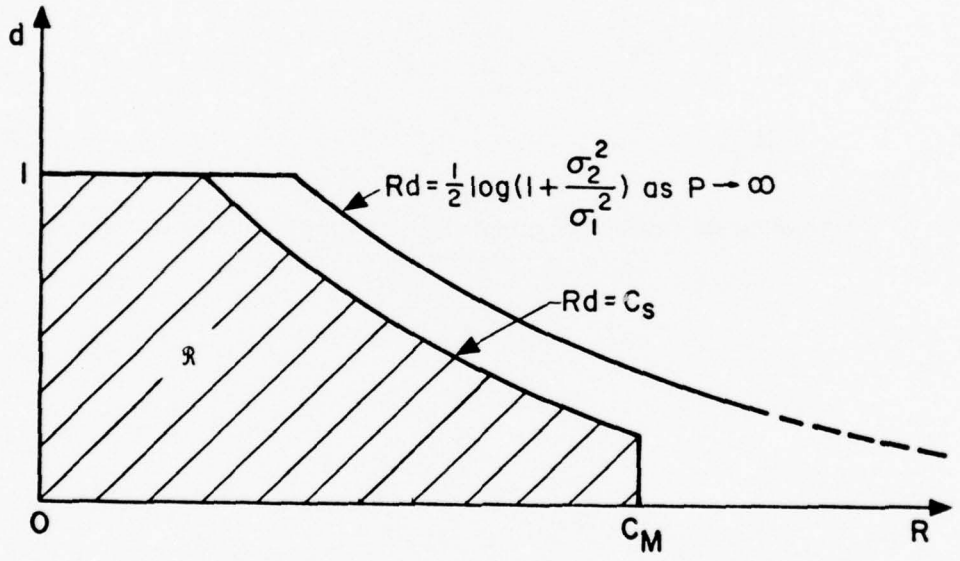


Figure 2.5 - ACHIEVABLE REGION FOR THE GAUSSIAN WIRETAP CHANNEL

Recall from (2.1.13) that

$$C_s = C_M - C_{MW} \tag{2.4.1}$$

$$= \frac{1}{2}\log\left(1 + \frac{P}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1 + \frac{P}{\sigma_1^2 + \sigma_2^2}\right) \tag{2.4.2}$$

$$= \frac{1}{2}\log\left[\left(\frac{P + \sigma_1^2}{P + \sigma_1^2 + \sigma_2^2}\right)\left(1 + \frac{\sigma_2^2}{\sigma_1^2}\right)\right]. \tag{2.4.3}$$

Theorem 2.2 shows that C_s almost completely characterizes the achievable (R,d) region. It is easy to see that C_s increases monotonically as the power constraint P is relaxed. The limiting value of C_s for very large P is $\frac{1}{2} \log (1 + \frac{\sigma_2^2}{\sigma_1^2})$.

In the power limited region $(P << \sigma^2)$

$$C_M \doteq P/(\sigma_1^2\ 2\ell n\ 2) \tag{2.4.4}$$

$$C_{MW} \doteq P/[(\sigma_1^2 + \sigma_2^2)\ 2\ell n\ 2] \tag{2.4.5}$$

and

$$C_s/C_M \doteq \sigma_2^2/(\sigma_1^2 + \sigma_2^2). \tag{2.4.6}$$

In the bandwidth limited region $(P >> \sigma^2)$

$$C_M \doteq 1/2 \log (P/\sigma_1^2) \tag{2.4.7}$$

$$C_{MW} \doteq 1/2 \log [P/(\sigma_1^2 + \sigma_2^2)] \tag{2.4.8}$$

so that

$$C_s \doteq 1/2 \log [(\sigma_1^2 + \sigma_2^2)/\sigma_1^2] \tag{2.4.9}$$

and

$$C_s/C_M \doteq 0. \tag{2.4.10}$$

Our results are therefore of most use on power limited channels. Of course if the main channel is bandwidth limited $(P/\sigma_1^2 >> 1)$ and the wiretap channel is power limited $(P/(\sigma_1^2 + \sigma_2^2) << 1)$ then C_s/C_M will be even closer to 1. It is really only the wiretap channel which must be power limited.

A certain amount of caution should be exercised when using theorem 2.2. Our results were derived on the assumption that we had perfect knowledge of the main channel and wiretap channel noise statistics. In practice the signal to noise ratios (SNR) on the channels may be somewhat uncertain. In this case the system may be operating several dB below the actual capacity of the main channel, and if the wiretap channel's SNR is less than this amount below the main channel's SNR then secrecy is lost.

But in spite of these problems there may be practical applications for these results. If, for example, the wiretapper is listening to unintentional electromagnetic radiation from a terminal or computer, his SNR may be tens of dB down from that of the "main channel". Such a wiretap channel allows almost no reduction in rate of information flow to be coupled with high uncertainty on the part of the wiretapper.

2.4.2 THE GENERAL DISCRETE MEMORYLESS WIRETAP CHANNEL

As mentioned in the previous section, the complete set of achievable (R,d) pairs for the Gaussian wiretap channel is characterized by the secrecy capacity C_s. Such channels (which we will refer to as constant $\Gamma(R)$ channels) have the property that time-sharing can be used to obtain the whole achievable region from the achievability of the two extreme points. In this section, we will use Wyner's basic result for discrete memoryless wiretap channels to deduce a useful characterization of constant $\Gamma(R)$ wiretap channels. Examples of

such channels and others are given.

The reason for referring to channels characterized by the secrecy capacity C_s as constant $\Gamma(R)$ channels follows from theorem 2.1. We recall that

$$\Gamma(R) = \max_{p_X \in \rho(R)} I(X;Y|Z) \tag{2.4.11}$$

where $p_X(\cdot)$ is a probability distribution on the input of the main channel and $\rho(R)$ is the set of p_X such that $I(X;Y) \geq R$. We can rewrite $I(X;Y|Z)$ as

$$I(X;Y|Z) = H(X|Z) - H(X|Y,Z) \tag{2.4.12}$$

$$= H(X|Z) - H(X|Y) \tag{2.4.13}$$

$$= I(X;Y) - I(X;Z) \tag{2.4.14}$$

where in (2.4.13) we have used the fact that X,Y and Z form a Markov chain.

Theorem 2.5

$\Gamma(R)$ is constant if and only if p_X^* maximizes $I(X;Y) - I(X;Z)$ where p_X^* is a capacity achieving distribution on the main channel.

Proof:

If p_X^* maximizes $I(X;Y) - I(X;Z)$, then

$$\Gamma(R) = I_{p_X^*}(X;Y) - I_{p_X^*}(X;Z) \tag{2.4.15}$$

since $p_X^* \in \rho(R)$ for $0 \leq R \leq C_M$. Therefore $\Gamma(R)$ is a constant.

Conversely, suppose p_X^* does not maximize $I(X;Y) - I(X;Z)$. Let the maximizing distribution be denoted by p_X', and let $I_{p_X'}(X;Y) = R_1$. Then, it is clear that $\Gamma(R_1) > \Gamma(C_M)$. This shows that $\Gamma(R)$ cannot be a constant. □

We have already seen two examples of constant $\Gamma(R)$ channels, namely the Gaussian wiretap channel and the simple channel of figure 2.2. Some more examples are given in Appendix III. Here we look at a channel for which $\Gamma(R)$ is not constant.

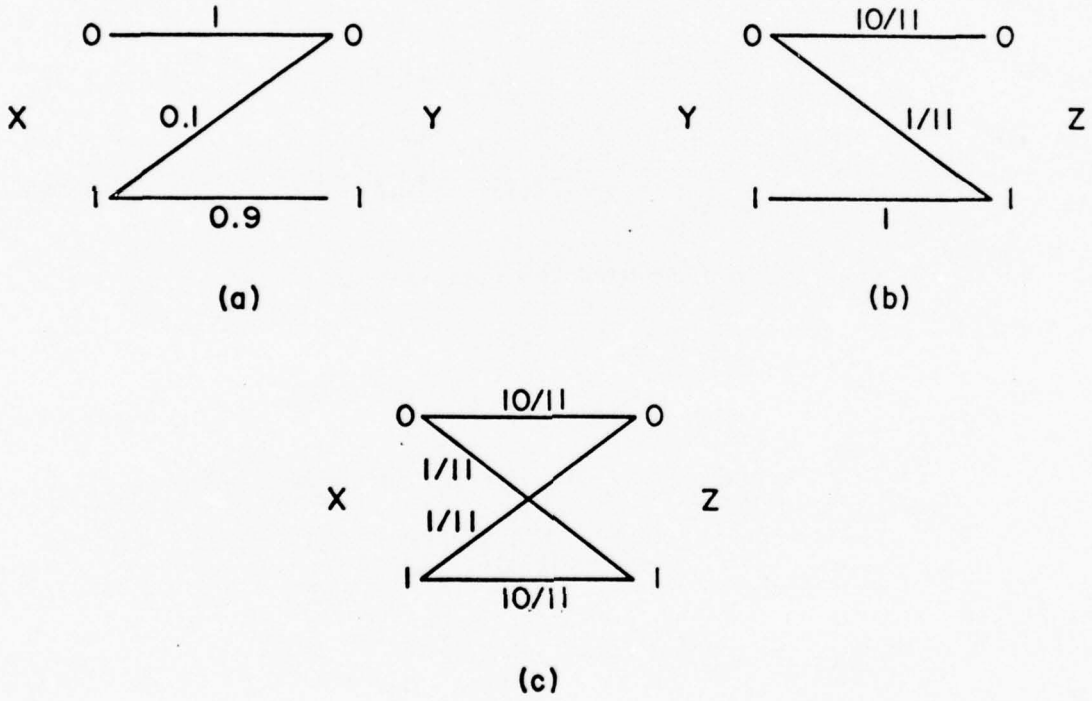


Figure 2.6

(a) Main channel
(b) Wiretap channel
(c) Cascade of main and wiretap channels

Referring to figure 2.1, consider the case in which the main and wiretap channels are as shown in figures 2.6(a) and 2.6(b) respectively. It can quite easily be verified that the cascade of these two channels is equivalent to a BSC with a crossover probability ε of $1/11$. We can evaluate the mutual informations between X and Y and X and Z to obtain

$$I(X;Y) = h(0.1 + 0.9q_0) - (1-q_0)\, h(0.1) \qquad (2.4.16)$$

$$I(X;Z) = h(\frac{1}{11} + \frac{9}{11}q_0) - h(\frac{1}{11}) \qquad (2.4.17)$$

where $q_0 = \Pr\{X = 0\}$ and $h(\cdot)$ is the binary entropy function.

Figure 2.7 shows a plot of $I(X;Y)$ and $I(X;Z)$ against q_0. The maximum of $I(X;Y)$ occurs at $q_0 = 0.54$ and equals 0.76. By definition, this value is also the capacity C_M of the main channel. Because of the symmetry of the channel from X to Z, $I(X;Z)$ is maximized at $q_0 = 0.5$. The interesting point to note is that the difference between $I(X;Y)$ and $I(X;Z)$ is maximized at $q_0 = 0.69$ which corresponds to a value for $I(X;Y)$ of 0.71. The fact that $r(R)$ is not constant is illustrated in figure 2.8.

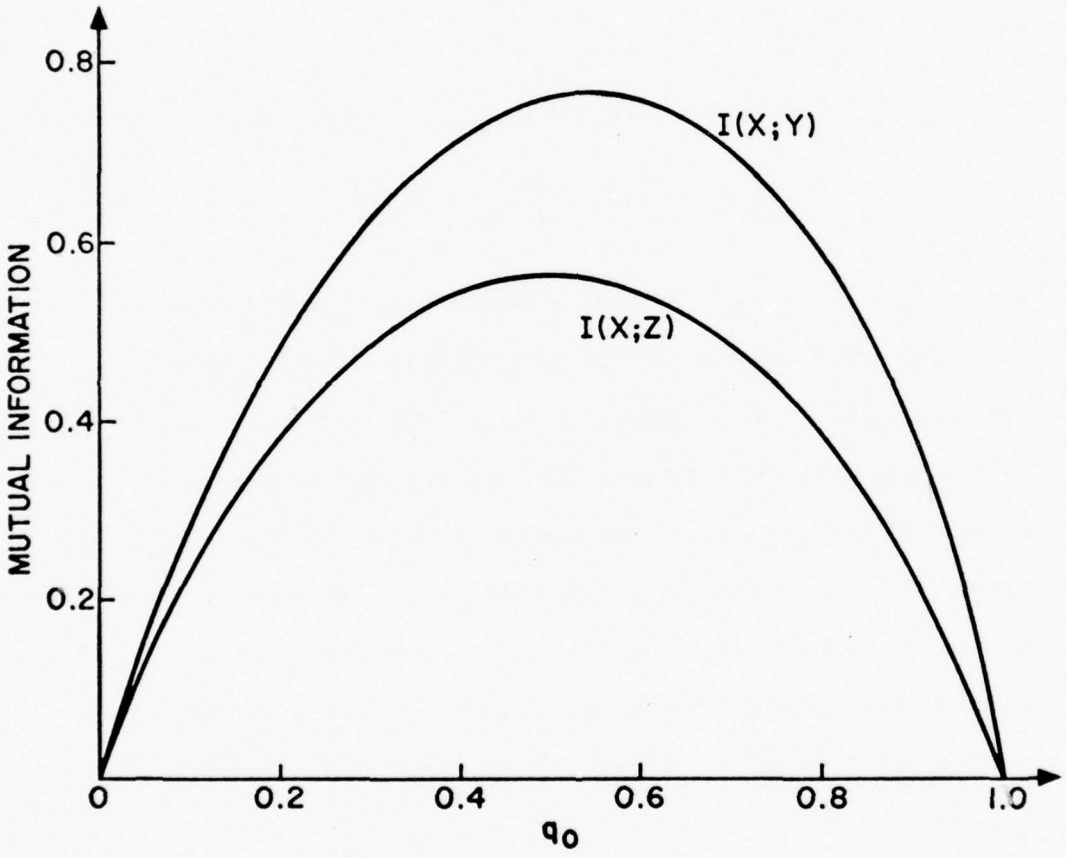


Figure 2.7 - PLOT OF I(X;Y) and I(X;Z) AGAINST INPUT PROBABILITY DISTRIBUTION FOR EXAMPLE OF FIGURE 2.6

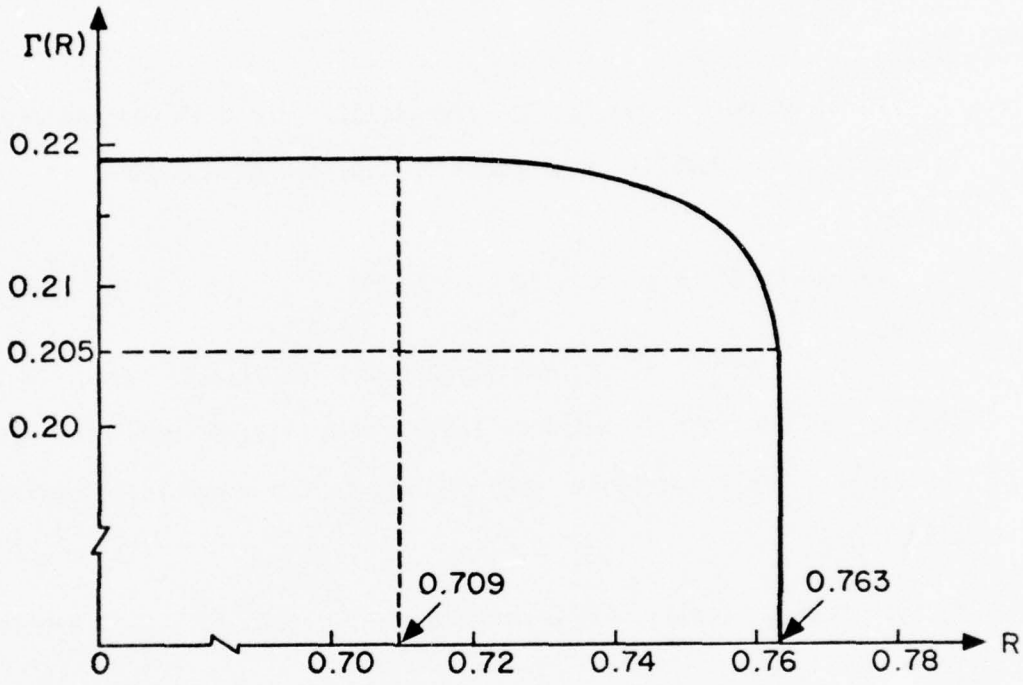


Figure 2.8 - Γ(R) FOR THE WIRETAP CHANNEL EXAMPLE OF FIGURE 2.6.

We now give a necessary condition for Γ(R) to be constant for a special class of discrete memoryless wiretap channels.

Lemma 2.11

Let the main channel be a discrete memoryless channel (DMC) with K inputs, and the wiretap channel be some other DMC. Suppose that I(X;Y) is maximized at a unique input distribution $p_X^* = (p^*(1), p^*(2), \ldots, p^*(K))$ where all the components of p_X^* are strictly positive.

Then a necessary condition for $\Gamma(R)$ to be constant is that $p_X^\star$ should be a maximizing distribution for $I(X;Z)$.

Proof:

First we note that $I(X;Y)$ and $I(X;Z)$ are both concave functions of the input probability assignment p_X to the main channel [3, theorem 4.4.2].

We can handle the equality constraint $\sum_{i=1}^{K} p(i) = 1$ by substituting $1 - \sum_{i=1}^{K-1} p(i)$ for $p(K)$ in the expressions for $I(X;Y)$ and $I(X;Z)$. Thus we can consider maximizing $I(X;Y)$ and $I(X;Z)$ which are now functions of $K-1$ variables subject only to the inequality constraints $p(i) \geq 0$.

By hypothesis, $I(X;Y)$ has a maximum at $p_X^\star$ and $p_X^\star > 0$. Therefore, [24]

$$\left.\frac{\partial I(X;Y)}{\partial p(i)}\right|_{p_X^\star} = 0, \quad 1 \leq i \leq K - 1. \tag{2.4.18}$$

Now assume that $p_X^\star$ does not maximize $I(X;Z)$. Then there exists at least one $j \in [1, K-1]$ such that

$$\left.\frac{\partial I(X;Z)}{\partial p(j)}\right|_{p_X^\star} \neq 0 \tag{2.4.19}$$

Thus, by moving away from $p_X^\star$ along the direction of $p(j)$[†], the

[†]Note that this is always possible since we assumed that all the components of $p_X^\star$ are strictly positive.

difference between $I(X;Y)$ and $I(X;Z)$ can be made to increase (at least initially). Therefore, p_X^* does not maximize $I(X;Y) - I(X;Z)$ and by theorem 2.5, this implies that $r(R)$ is not constant. □

Remark:

Lemma 2.11 can be extended in a straight forward manner to cover the case where $I(X;Y)$ is maximized at non-unique but strictly positive input distributions.

Corollary 1:

Under the assumptions of lemma 2.11, if $r(R)$ is a constant, then

$$r(R) = C_M - C_{MW} \tag{2.4.20}$$

where

$$C_M = \max_{p_X} I(X;Y) \tag{2.4.21 a}$$

and

$$C_{MW} = \max_{p_X} I(X;Z) \tag{2.4.21 b}$$

Proof:

$$r(R) = \max_{p_X \varepsilon \rho(R)} [I(X;Y) - I(X;Z)] \tag{2.4.22}$$

Since $r(R)$ is a constant, we have

$$r(R) = r(C_M) \tag{2.4.23}$$

$$= I_{p_X^*}(X;Y) - I_{p_X^*}(X;Z) \tag{2.4.24}$$

$$= C_M - C_{MW} \tag{2.4.25}$$

where in (2.4.25) we have used lemma 2.11 to obtain $I^{*}_{p_X}(X;Z) = C_{MW}$. □

Corollary 2:

$\Gamma(R)$ is not constant for the wiretap channel example of figure 2.6.

2.4.3 NON-DEGRADED WIRETAP CHANNELS

Thus far we have modeled the wiretapper's channel as a degraded form of the main channel. While this model is very suggestive and often arises in practical situations, there may be situations in which the notion of degradation is not applicable. We now give an example of a very simple non-degraded wiretap channel in which the "main channel" can be operated at capacity whilst the wiretapper can be kept totally ignorant of the intended message.

The example is the orthogonal broadcast channel [4] shown in figure 2.9. The connecting lines denote transition probabilities of 1. For simplicity, let us assume that the source is binary symmetric. We can send reliably to Y (the legitimate receiver) at the maximum possible rate of 1 bit per channel use whilst keeping Z (the wiretapper) totally ignorant of the source output, by using only the two input letters labelled 1 and 3. If the source output is 0, a '1' is transmitted. Otherwise a '3' is sent. It can easily be seen that this scheme achieves a point $(R,d) = (1,1)$.

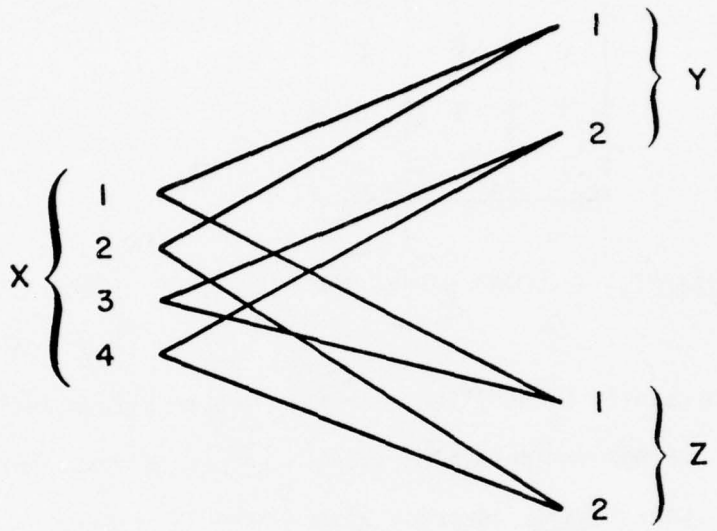


Figure 2.9 - NON-DEGRADED WIRETAP CHANNEL

It may seem that somehow the above scheme is not making full use of the capabilities of the channel. If we consider Y and Z to be two receivers which are to learn only the messages specifically destined for them and not each other's message, we can use the coding scheme shown in Table 2.1. S_1 and S_2 are the source outputs of two independent binary symmetric sources which are to be sent to Y and Z respectively.

S_1	S_2	X
0	0	1
0	1	2
1	0	3
1	1	4

Table 2.1 - CODING SCHEME FOR CHANNEL OF FIGURE 2.9.

It can readily be verified that this scheme allows reliable transmission at the maximum possible rates to both receivers, but each receiver is kept totally ignorant of the other's message.

The privacy problem can be extended to networks. We might mention a two-sender, two-receiver network in which each sender wishes to communicate reliably with its intended receiver while keeping the other receiver as ignorant as possible of the message. The problem now consists of four parameters of interest:

R_i, $i = 1, 2$, the transmission rate to receiver i from sender i.

d_i, $i = 1, 2$, the equivocation about the message intended for the other receiver at receiver i.

CHAPTER 3

THE WIRETAP CHANNEL WITH FEEDBACK

3.1 INTRODUCTION

In the previous chapter, we examined the Gaussian wiretap channel which is included in the class of degraded wiretap channels (i.e. the wiretapper's data is a degraded version of the legitimate receiver's data). This class of channels possesses a certain symmetry between the legitimate receiver and the wiretapper: both are just observers of the data coming over their respective channels. If the two channels are statistically equivalent, then the legitimate receiver is no better off than the wiretapper and no rate-equivocation pair (R,d) such that $Rd>0$ can be achieved. Therefore the approach taken in chapter 2 (except for section 2.4.3) is suited for channels in which it is known that the wiretapper's channel is a degraded form of the main channel.

In practice this would hopefully be the case. However, there may be situations in which the wiretapper's channel is as good as or maybe even better than the main channel. In this case, the only hope remaining to confuse the wiretapper is to destroy the symmetry mentioned earlier. Here we will consider one way of achieving this, namely by allowing feedback from the legitimate receiver.

The model which we wish to analyze is shown in figure 3.1. Unlike figure 2.1 where the input to the wiretap channel is the output of the main channel, we now allow the wiretapper to view the output of the encoder directly through his channel. The decoder at the legitimate receiver is permitted to send back information to the encoder through a noiseless, infinite-capacity feedback link. The wiretapper is not allowed to inject

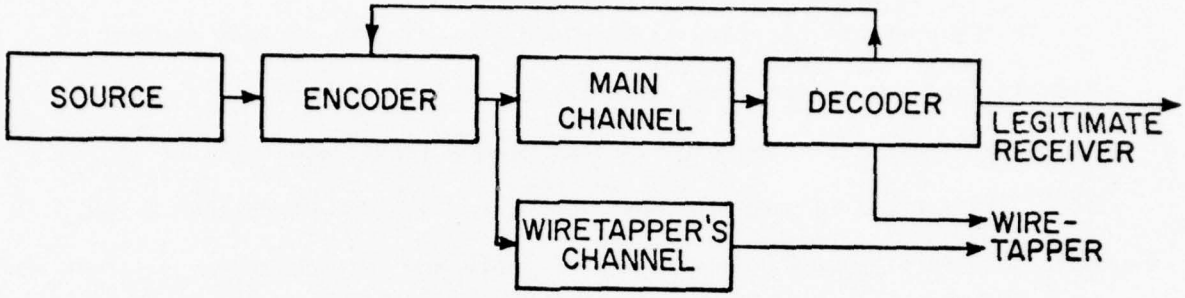


Figure 3.1 - MODEL FOR WIRETAP CHANNEL WITH FEEDBACK

data into the feedback channel even though he might wish to do so in an attempt to mislead or confuse the encoder. This would be a good model for the practical situation in which the wiretapper does not wish to make his presence known.

If the feedback link is private (i.e. the wiretapper cannot gain access to the data which is fed back) a one-time pad cryptographic system [18, 31] could be used to achieve $R = C_M$, $d = 1$. That is, data could be sent to the legitimate receiver at the maximum possible rate consistent with reliable communication and at the same time the wiretapper could be completely foiled. To accomplish this, the decoder sends back a totally random sequence independent of all else, which the encoder exclusive-ors with the data to be transmitted. The random sequence is subtracted out at the legitimate receiver and so does not affect the rate

of reliable transmission. But it acts as a totally noisy channel as far as the wiretapper is concerned.

For the remainder of this chapter, we consider the harder problem in which the feedback link is public, i.e. any data fed back from the legitimate receiver to the encoder is available to the wiretapper. We now focus our attention on an interesting wiretap channel with feedback and derive inner and outer bounds on the achievable (R,d) region.

3.2 THE BINARY ERASURE WIRETAP CHANNEL

3.2.1 AN ACHIEVABLE RATE-EQUIVOCATION REGION

The model of the binary erasure wiretap channel is as shown in figure 3.1 with the main and wiretapper's channels being independent binary erasure channels of erasure rates ε_1 and ε_2 respectively. For simplicity, we shall assume that the source is binary symmetric.

We shall first prove the following result which establishes an innerbound on the achievable (R,d) region.

Theorem 3.1

The set of (R,d) pairs defined by

$$R \leq (1-\varepsilon_1) = C_M \tag{3.2.1}$$

$$d \leq 1 \tag{3.2.2}$$

$$Rd \leq \frac{\varepsilon_2(1-\varepsilon_1)^2}{1-\varepsilon_1\varepsilon_2} \tag{3.2.3}$$

is achievable.

We shall establish theorem 3.1 by showing that the extreme points

$$(R_1,d_1) = (1-\varepsilon_1,\ \varepsilon_2(1-\varepsilon_1)/(1-\varepsilon_1\varepsilon_2)) \tag{3.2.4}$$

and

$$(R_2,d_2) = (\varepsilon_2(1-\varepsilon_1)^2/(1-\varepsilon_1\varepsilon_2)\ ,\ 1) \tag{3.2.5}$$

are achievable. We can then invoke the time sharing argument of lemma 2.1 to conclude that the entire region defined in theorem 3.1 is achievable.

The point (R_1,d_1) can be achieved using the following scheme. The source outputs are sent directly over the channels with no encoding. Whenever the legitimate receiver gets an erasure, he asks for a retransmission until he learns the bit being transmitted. Thus his probability of decoding error will be zero. The probability that a bit sent over the main channel will result in an erasure is ε_1. Therefore the number of channel uses required for a successful transmission has a geometric distribution with parameter $1-\varepsilon_1$ and the expected number of channel uses per bit is $1/(1-\varepsilon_1)$.

If we consider transmitting a long sequence of source outputs over the main channel, the transmission rate R_1 will be $(1-\varepsilon_1)$ bits/channel use.

Let us now calculate the equivocation d_1 of the wiretapper resulting from this coding scheme. Clearly,

$$d_1 = \Pr\{\text{wiretapper misses a bit}\} \tag{3.2.6}$$

$$= \Pr\{\text{main channel output shows a non-erasure bit } \underline{\text{before}} \text{ wiretapper's channel output}\} \tag{3.2.7}$$

$$= \varepsilon_2(1-\varepsilon_1) + \varepsilon_2^2\varepsilon_1(1-\varepsilon_1) + \varepsilon_2^3\varepsilon_1^2(1-\varepsilon_1)+\ldots + \varepsilon_2^i\varepsilon_1^{i-1}(1-\varepsilon_1) + \ldots \tag{3.2.8}$$

$$= \varepsilon_2(1-\varepsilon_1) \sum_{i=0}^{\infty} (\varepsilon_1\varepsilon_2)^i \tag{3.2.9}$$

$$= \varepsilon_2(1-\varepsilon_1)/(1-\varepsilon_1\varepsilon_2) \tag{3.2.10}$$

Thus,

$$d_1 = \varepsilon_2(1-\varepsilon_1)/(1-\varepsilon_1\varepsilon_2) \tag{3.2.11}$$

and this proves that (R_1,d_1) is achievable.

To complete the proof of theorem 3.1, we need to show that (R_2,d_2) is also achievable. Suppose we wish to transmit k source outputs reliably to the legitimate receiver. Then we are allowed k/R_2 channel uses where $R_2 = \varepsilon_2(1-\varepsilon_1)^2/(1-\varepsilon_1\varepsilon_2)$. But on the average, the successful transmission of 1 bit of information to the legitimate receiver requires $1/(1-\varepsilon_1)$ channel uses. Therefore in k/R_2 channel uses, we can reliably transmit $k(1-\varepsilon_1)/R_2 = k(1-\varepsilon_1\varepsilon_2)/\varepsilon_2(1-\varepsilon_1)$ bits of information. (Note that the *preceeding argument is not strictly rigorous.* For example, to be precise we should have stated that as $k\to\infty$, the probability that we can transmit $k\{[(1-\varepsilon_1)/R_2]-\delta\}$ bits in k/R_2 channel uses tends to 1 for every $\delta>0$. We omit these details in order to simplify the proof. This remark will also apply to some subsequent arguments in this section).

The idea now is to tag on $k[\frac{(1-\varepsilon_1)}{R_2} - 1]^{\dagger}$ totally random bits to the k source outputs. An invertible prescrambling operation similar to that of Hellman and Carleial [20] is then used to obtain the codeword (of length $k(1-\varepsilon_1)/R_2$) to be transmitted. This prescrambling operation will be specified shortly and will be used to prove that the wiretapper can be kept totally ignorant of the k source outputs intended for the legitimate receiver. First we recall from (3.2.10) that

---

†If this is not an integer, a trivial modification is needed.

$$\Pr\{\text{wiretapper misses a bit}\} = \varepsilon_2(1-\varepsilon_1)/(1-\varepsilon_1\varepsilon_2). \tag{3.2.12}$$

So the number of bits in the codeword which the wiretapper misses is

$$[k(1-\varepsilon_1)/R_2]\ \varepsilon_2(1-\varepsilon_1)/(1-\varepsilon_1\varepsilon_2)$$
$$= k\ . \tag{3.2.13}$$

We now prove the following theorem which will establish the achievability of the point (R_2, d_2).

Theorem 3.2

Let $\underline{s}^k$ and $\underline{r}^{n-k}$ be independent, totally random binary column vectors. Let

$$\underline{x}^n = A\begin{pmatrix}\underline{s}\\ \underline{r}\end{pmatrix} \tag{3.2.14}$$

where A is chosen randomly and uniformly from the set of n x n invertible binary matrices. Suppose that $\underline{z}$ is equal to $\underline{x}$ except for k erasures. Then, over this ensemble of codes

$$\Pr\{A : H(\underline{S}|\underline{Z}) \geq k(1-\Delta)\} = 1-\delta(n) \tag{3.2.15}$$

for all $\Delta > 0$. The symbol $\delta(n)$ stands for some quantity which tends to 0 as $n \to \infty$.

Proof:

Using $H(A) + H(B|A) = H(B) + H(A|B)$ we find that

$$H(\underline{S}|\underline{Z}) = H(\underline{S}) + H(\underline{Z}|\underline{S}) - H(\underline{Z}) \tag{3.2.16}$$
$$= H(\underline{S}) + [H(\underline{X}|\underline{S}) + H(\underline{Z}|\underline{X},\underline{S}) - H(\underline{X}|\underline{Z},\underline{S})] - H(\underline{Z}) \tag{3.2.17}$$

Since A is an invertible matrix we have

$$H(\underline{X}|\underline{S}) = n-k \tag{3.2.18}$$

Also since $\underline{x}$ completely determines $\underline{s}$,

$$H(\underline{Z}|\underline{X},\underline{S}) = H(\underline{Z}|\underline{X}) \tag{3.2.19}$$

Therefore,

$$H(\underline{Z}) - H(\underline{Z}|\underline{X},\underline{S}) = I(\underline{X};\underline{Z}) \tag{3.2.20}$$

$$= n-k \tag{3.2.21}$$

Using (3.2.18) and (3.2.21) in (3.2.17) yields

$$H(\underline{S}|\underline{Z}) = H(\underline{S}) - H(\underline{X}|\underline{Z},\underline{S}) \tag{3.2.22}$$

The proof of theorem 3.2 is completed by applying lemma 3.1.

Lemma 3.1

$$\Pr\{A : H(\underline{X}|\underline{Z},\underline{S}) \leq \ell\} \geq 1-2^{-\ell} \tag{3.2.23}$$

Proof:

From (3.2.14) we have

$$\begin{pmatrix} \underline{s} \\ \underline{r} \end{pmatrix} = A^{-1}\,\underline{x} = B\,\underline{x} \tag{3.2.24}$$

where $B = \begin{pmatrix} \underline{b}_1^T \\ \vdots \\ \underline{b}_n^T \end{pmatrix}$ has the same distribution as A.

With no loss of generality, let us assume that the last k bits of $\underline{z} = (z_1, z_2, \ldots, z_n)$ are erasures, i.e.,

$$\begin{aligned} z_1 &= x_1 \\ z_2 &= x_2 \\ &\vdots \\ z_{n-k} &= x_{n-k} \,. \end{aligned} \tag{3.2.25}$$

We know that

$$\begin{aligned} s_1 &= \underline{b}_1^T\,\underline{x} \\ s_2 &= \underline{b}_2^T\,\underline{x} \\ &\vdots \\ s_k &= \underline{b}_k^T\,\underline{x} \end{aligned} \tag{3.2.26}$$

where $\underline{b}_i$ is chosen uniformly from all binary n-vectors not in the span of

$\{\underline{b}_1, \underline{b}_2, \ldots, \underline{b}_{i-1}\}$, and $\underline{b}_1$ is chosen uniformly from all non-zero n-vectors. Now

$$H(\underline{X}|\underline{Z},\underline{S}) = n - \text{rank } M_1 \tag{3.2.27}$$

where

$$M_1 = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & & & \\ 0 & 0 & .. 1 & .. 0 \\ & \underline{b}_1^T & & \\ & \vdots & & \\ & \underline{b}_k^T & & \end{bmatrix} \begin{matrix} \uparrow \\ \\ n-k \\ \downarrow \\ \\ \uparrow \\ k \\ \downarrow \end{matrix} \quad . \tag{3.2.28}$$

Let us define a matrix M_2 as

$$M_2 = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & & & \\ 0 & 0 & .. 1 & .. 0 \\ & \underline{c}_1^T & & \\ & \vdots & & \\ & \underline{c}_k^T & & \end{bmatrix} \begin{matrix} \uparrow \\ \\ n-k \\ \downarrow \\ \\ \uparrow \\ k \\ \downarrow \end{matrix} \tag{3.2.29}$$

where c_i^T , $1 \le i \le k$, is chosen uniformly from all binary n-vectors. It is intuitively clear that

$$\Pr\{\text{rank } M_1 \ge j\} \ge \Pr\{\text{rank } M_2 \ge j\} \; . \tag{3.2.30}$$

A rigorous proof is given in lemma 3.2. The probability that rank $M_2 \ge n-\ell$ for $0 \le \ell \le k-1$ is lower bounded by

$$\frac{2^n - 2^{n-k}}{2^n} \cdot \frac{2^n - 2^{n-k+1}}{2^n} \cdots \cdot \frac{2^n - 2^{n-\ell-1}}{2^n} \tag{3.2.31}$$

$$= (1 - 2^{-k})(1 - 2^{-k+1}) \ldots (1 - 2^{-\ell-1}) \tag{3.2.32}$$

$$> (1 - 2^{-\ell-1})\,(1 - 2^{-\ell-2}) \ldots \tag{3.2.33}$$

$$\geq 1 - 2^{-\ell}\,. \tag{3.2.34}$$

where in (3.2.34) we have used the fact that

$$\prod_{i=1}^{n} (1 - \alpha_i) \geq 1 - \sum_{i=1}^{n} \alpha_i\,, \quad \alpha_i \geq 0. \tag{3.2.35}$$

From (3.2.30) we conclude that

$$\Pr\{\text{rank } M_1 \geq n-\ell\} \geq 1 - 2^{-\ell} \tag{3.2.36}$$

and using (3.2.27) we obtain the desired result, i.e.,

$$\Pr\{A : H(\underline{X}|\underline{Z},\underline{S}) \leq \ell\} \geq 1 - 2^{-\ell}. \tag{3.2.37}$$

Lemma 3.2

$$\Pr\{\text{rank } M_1 \geq j\} \geq \Pr\{\text{rank } M_2 \geq j\} \tag{3.2.38}$$

Proof:

Let us choose the $\{\underline{b}_i\}$ and $\{\underline{c}_i\}$ as follows:
We first choose $\underline{c}_1 \sim U\{0, 1\}^n$ i.e., according to a uniform distribution on $\{0, 1\}^n$. If $\underline{c}_1 \neq \underline{0}$, then $\underline{b}_1 = \underline{c}_1$. Otherwise, we choose again until we obtain a non-zero $\underline{b}_1$. In general, we choose $\underline{c}_i \sim U\{0, 1\}^n$ and if $\underline{c}_i$ is not in the span of $\{\underline{b}_1, \ldots, \underline{b}_{i-1}\}$, then $\underline{b}_i = \underline{c}_i$. Otherwise, we draw again until we get a $\underline{b}_i \notin$ span $\{\underline{b}_1, \ldots, \underline{b}_{i-1}\}$. Thus we conclude that the span of $\{\underline{b}_1, \ldots, \underline{b}_k\}$ is at least as large as the span of $\{\underline{c}_1, \ldots, \underline{c}_k\}$. □

3.2.2 DISCUSSION OF ACHIEVABLE REGION

In this section we shall discuss some of the implications of theorem 3.1. We examine three separate cases.

Case I: $\varepsilon_1 = \varepsilon_2 = \varepsilon$.

In this case, theorem 3.1 states that the region defined by $R \leq 1-\varepsilon$, $d \leq 1$ and $Rd \leq \varepsilon(1-\varepsilon)/(1+\varepsilon)$ can be achieved. If $\varepsilon = 0.5$ and $d = 1$, then a rate of 0.5/3 is achievable. This means that even though the wiretapper's channel is as good as that of the legitimate receiver, feedback allows totally secure transmission up to a rate at least equal to a third of the main channel capacity. A plot of $\varepsilon(1-\varepsilon)/(1+\varepsilon)$ as a function of ε is sketched in figure 3.2.

Case II: $\varepsilon_1 = 0$, $\varepsilon_2 = \varepsilon$.

Here the region which can be achieved is given by $R \leq 1$, $d \leq 1$, $Rd \leq \varepsilon$. This is the situation in which the main channel is noiseless and from Appendix II, we know that when no feedback is allowed, the set of all achievable (R,d) pairs is identical to the region defined above. This is really not very surprising as will be shown in the next section.

Case III: $\varepsilon_1 = 0.5$, $\varepsilon_2 = \varepsilon$.

The achievable region is now lowerbounded by $R \leq 0.5$, $d \leq 1$, $Rd \leq \varepsilon/(4-2\varepsilon)$. Figure 3.3 shows a plot of $\varepsilon/(4-2\varepsilon)$ as a function of ε.

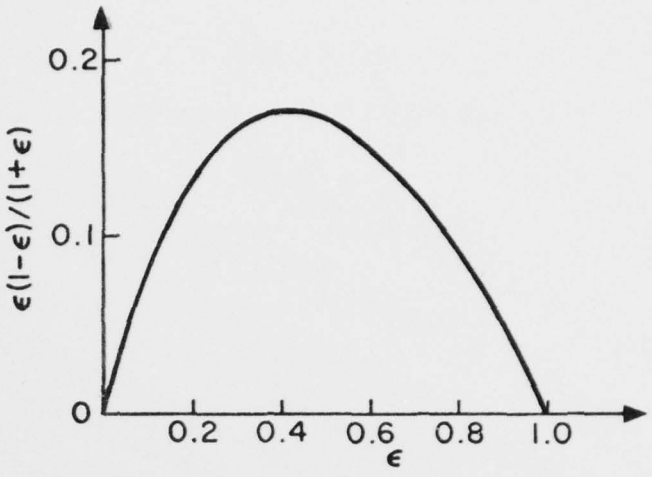


Figure 3.2 - PLOT OF $\varepsilon(1-\varepsilon)/(1+\varepsilon)$ AGAINST ε

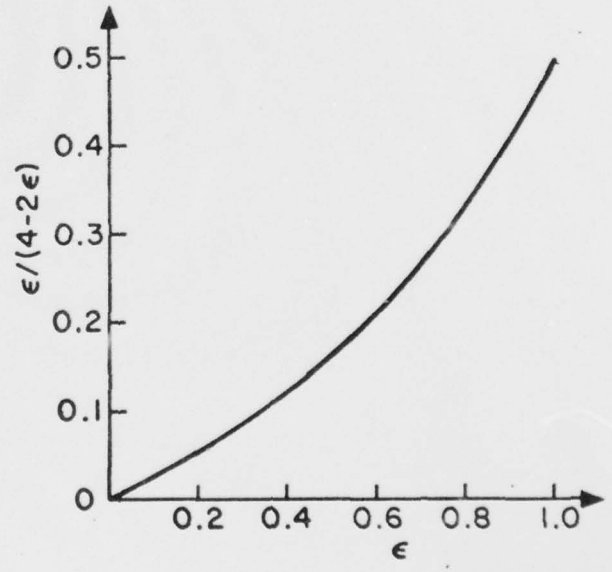


Figure 3.3 - PLOT OF $\varepsilon/(4-2\varepsilon)$ AGAINST ε

We might also point out that as long as $\varepsilon_1 < 1$ and $\varepsilon_2 > 0$, it is possible to transmit at a positive rate in perfect secrecy.

3.2.3. AN OUTERBOUND ON THE ACHIEVABLE RATE-EQUIVOCATION REGION

We shall develop an outerbound for the binary erasure wiretap channel with feedback. The generalization of this outerbound to channels with D-ary input and E-ary output alphabets is easy.

Theorem 3.3

The set $\mathcal{R}_1$ of all (R, d) pairs which can be achieved on the binary erasure channel with feedback is contained in the set of all achievable (R, d) pairs when the main channel is made noiseless and no feedback is allowed.

Remark: In general, the main channel is made into a noiseless channel with M-ary input and output alphabets where $M = \min \{D, E\}$.

Proof: follows from lemmas 3.3 and 3.4.

Lemma 3.3

The set $\mathcal{R}_1$ defined in theorem 3.3 expands if the main channel is replaced by a noiseless binary channel.

Proof:

The original binary erasure wiretap channel can be recovered by cascading a binary erasure channel of erasure rate ε_1 with the noiseless channel. □

Lemma 3.4

If the main channel is noiseless, feedback cannot increase the achievable (R, d) region.

Proof:

Since the main channel is noiseless, the encoder knows exactly the data received by the legitimate receiver. Therefore the feedback information should not depend on this data since otherwise we would be needlessly allowing the wiretapper to gain extra information. Any "feedback information" could hence have been conveyed to both legitimate receiver and wiretapper prior to using the channel, and can be considered to be part of the code. The feedback link is thus unnecessary. □

Remark:

This lemma explains the results of case II in section 3.2.2.

When the main channel is "not very noisy", theorem 3.3 will yield a fairly tight outerbound. Unfortunately, for "noisy" main channels, we expect this bound to be very weak. The proof of a tight outerbound remains an open problem.

CHAPTER 4

FEEDBACK IN MULTIPLE-ACCESS CHANNELS

4.1 INTRODUCTION

This chapter is concerned with the use of noiseless feedback to improve the performance of communication systems. We begin with a brief review of some results concerning single-input single-output channels (see figure 1.1). In certain communication problems, a noiseless feedback link is available and may be used to improve communication over a noisy forward link. An example is communication with a satellite: the power in the ground-to-satellite direction is usually so much larger than in the reverse direction that the first link can be considered to be essentially noiseless.

One would expect that the use of the feedback link should somehow facilitate the task of sending information from the source to the destination. Therefore, Shannon's result [25, theorem 6] that the capacity of a memoryless forward channel is not increased by noiseless feedback is quite surprising. However, it is possible to take advantage of feedback to reduce decoding delay and system complexity [26].

More recently, Gaarder and Wolf [27] showed by an example that it is possible to increase the capacity region of a discrete memoryless multiple-access channel through the use of feedback. The example which they used is the noiseless binary erasure multiple-access channel shown in figure 4.1.

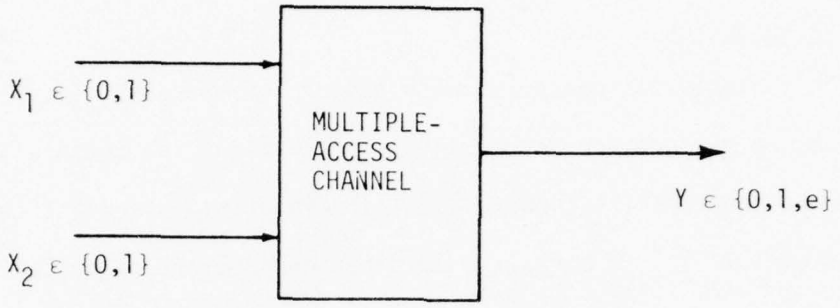


Figure 4.1 - NOISELESS BINARY ERASURE MULTIPLE-ACCESS CHANNEL

The transition probabilities for the channel are indicated in table 4.1.

		Y	
X_1X_2	0	1	e
0 0	1	0	0
0 1	0	0	1
1 0	0	0	1
1 1	0	1	0

Table 4.1 - TRANSITION PROBABILITIES FOR NOISELESS BINARY ERASURE MULTIPLE-ACCESS CHANNEL

Using the results of section 1.4 (specifically (1.4.2)) we find that the capacity region for the above channel without feedback is

$$\mathcal{C} = \{(R_1, R_2) \mid 0 \le R_1 \le 1,\ 0 \le R_2 \le 1,\ 0 \le R_1 + R_2 \le 1.5\} \qquad (4.1.1)$$

where R_i, i=1, 2 is the transmission rate from the ith transmitter. Gaarder and Wolf [27] show that the rate pair $(R_1, R_2) = (0.76, 0.76)$, which falls outside the region described in (4.1.1), is achievable.

Here we look at a feedback scheme for enlarging the capacity region of general multiple-access channels [28]. The scheme consists of two stages. During the first stage (stage 1), the two transmitters send information reliably to each other at the maximum possible rate. Stage 1 ends when each transmitter has complete knowledge of the other's message. Since each transmitter knows what it sent and sees the received data through the feedback link, this occurs before the receiver gains complete knowledge of the messages. That is, the rate of transmission in stage 1 will be too high for reliable transmission to the receiver. However, the stage 1 transmissions will enable the receiver to narrow down the set of possible transmitted messages to a considerably smaller set of "typical" messages. With probability arbitrarily close to 1, the set of "typical" messages will contain the actual transmitted message. The receiver and the two transmitters then arrange the messages in the "typical" set in some prearranged ordering. This sets up stage 2 during which the two transmitters totally cooperate to send the index of the actual transmitted message.

In retrospect, it is interesting to note that the scheme used by Gaarder and Wolf is a special case of the scheme proposed here.

Certain results and notations concerning multiple-access channels can be found in section 1.4 and will not be repeated here. We will show that the proposed feedback scheme increases the achievable rate region for the additive white Gaussian noise (AWGN) multiple-access channel. In section 4.4, we make a digression on typical sequences and recall some basic results which will be needed in section 4.5, where we consider discrete memoryless multiple-access channels. But first we introduce the model of the multiple-access channel with feedback and some additional notation.

4.2 FEEDBACK CHANNEL

The memoryless multiple-access channel with feedback is depicted in figure 4.2 below.

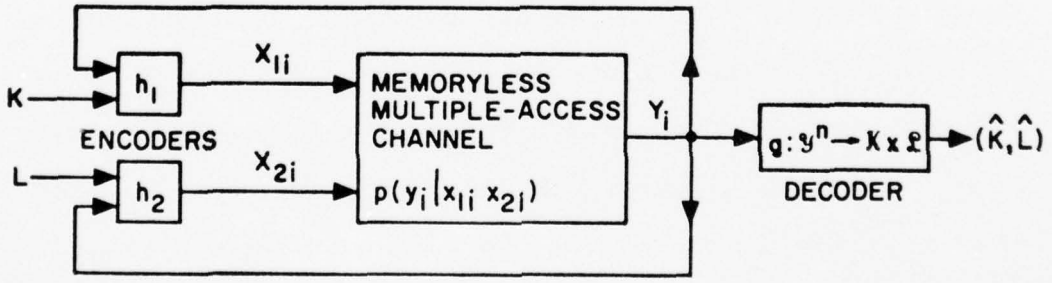


Figure 4.2 - MULTIPLE-ACCESS CHANNEL WITH FEEDBACK

The i^{th} symbol x_{1i} sent by transmitter 1 depends upon the message index k that transmitter 1 wishes to send and upon the previous receiver symbols $y_1, y_2, \ldots, y_{i-1}$. A similar statement holds for the i^{th} symbol x_{2i} sent by the second transmitter.

In the remainder of this chapter, the following notation will be used:

R_{12} = transmission rate from the first to the second transmitter during stage 1.

R_{21} = transmission rate from the second to the first transmitter during stage 1.

R_1 = overall (considering both stages) rate from the first transmitter to the receiver.

R_2 = overall rate from the second transmitter to the receiver.

4.3 THE AWGN MULTIPLE-ACCESS CHANNEL

For illustration, we will analyze in detail the symmetric case in which the average power constraints on both inputs are the same, namely $P_1 = P_2 = P$. We will then show how to generalize the scheme to the asymmetric case.

The basic idea is for each transmitter to send at full power to the receiver, but at rates corresponding to the capacity of the channel when the transmitter's own signal is subtracted out. Thus each transmitter very quickly learns what the other transmitter is sending. However, the receiver Y is still confused because the total rate has exceeded his capacity. In stage 2, the transmitters now use coherent transmission to send the missing bits in the receiver's knowledge of the intended messages.

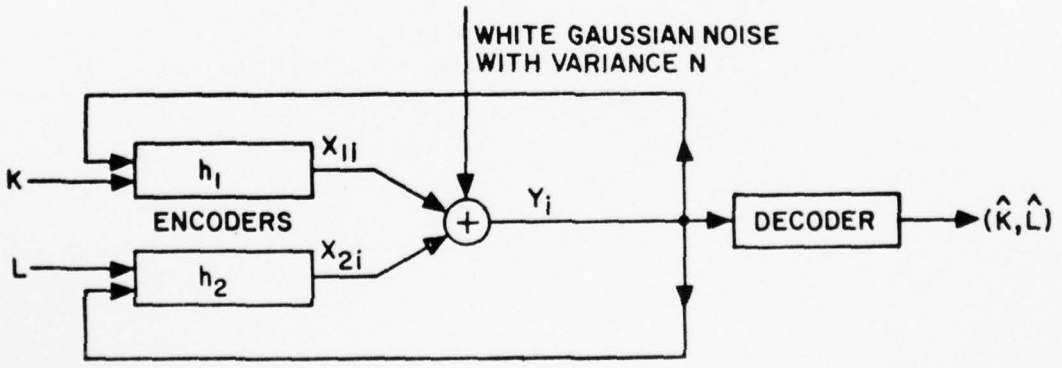


Figure 4.3 - AWGN MULTIPLE-ACCESS CHANNEL WITH FEEDBACK

The model for the AWGN multiple-access with feedback is shown in figure 4.3. Note that we are denoting the noise variance by N instead of σ^2 in order to simplify notation. Our proof that feedback can enlarge the achievable rate region makes use of the usual random coding argument. Consider the ensemble of randomly generated codes of blocklength n and rates $R_{12} = R_{21} = R^*$ obtained as follows. Each codeword $\underline{x}_1$ is an n-sequence of independent outcomes of a zero-mean Gaussian random variable with variance $P' = P-\eta$ where $\eta > 0$ is a quantity which will be made to tend to zero. We generate $2^{nR_{12}}$ independent such codewords. This will be the code used by the first transmitter during stage 1. Similarly the code used by the second transmitter during stage 1 is obtained by generating $2^{nR_{21}}$ independent codewords $\underline{x}_2$ as above.

Let us suppose that we wish to send one of 2^{nR^*} independent equiprobable messages to Y from each source. Because of the symmetry induced by the random coding, we can assume the messages actually transmitted to be (1, 1). From the results on coding for single-input single-output AWGN channels, we know that at the end of stage 1, $\underline{x}_1$ can be guessed at the second transmitter with arbitrarily small probability of error, say $P_{e_{1,2}} < \varepsilon/5$, $\varepsilon > 0$ if

$$R_{12} \leq \frac{1}{2} \log \left(1 + \frac{P'}{N}\right) \text{ bits/transmission} \qquad (4.3.1)$$

and the blocklength n is sufficiently large. Similarly, $\underline{x}_2$ can be estimated at the first transmitter with arbitrarily small probability of error, say $P_{e_{1,1}} < \varepsilon/5$, $\varepsilon > 0$ if

$$R_{21} \leq \frac{1}{2} \log \left(1 + \frac{P'}{N}\right) \text{ bits/transmission} \qquad (4.3.2)$$

and n is sufficiently large. In particular, we can set $R_{12} = R_{21} = R^* = \frac{1}{2} \log \left(1 + \frac{P'}{N}\right)$. We note that stage 1 requires n transmissions. Let us denote the n-sequence received at Y during stage 1 by $\underline{y}$. In the following, we shall be concerned with the set of 2^{2nR^*} codewords obtained by taking all possible sums $\underline{x} = \underline{x}_1 + \underline{x}_2$. By the independence of $\underline{x}_1$ and $\underline{x}_2$, each component of $\underline{x}$ is a zero-mean Gaussian r.v. with variance 2P'. We shall say that a codeword $\underline{x}$ is linked to $\underline{y}$ if $\underline{x}$ lies within the n-sphere of radius $\sqrt{n(N+\varepsilon)}$ centered at $\underline{y}$. By the law of large numbers, we know that with probability $P_c = 1 - \varepsilon/5$, $\varepsilon > 0$ the correct codeword will be linked to $\underline{y}$ for n sufficiently large.

We now proceed to consider the set $S_{\underline{y}}$ of codewords which, at the end of stage 1, are linked to $\underline{y}$. Let $|S_{\underline{y}}|$ denote the cardinality of $S_{\underline{y}}$. Then the average $|S_{\underline{y}}|$, taken over the ensemble of random codes and possible input messages is

$$E\,|S_{\underline{y}}| = 2L_1 + L_2 + P_c \tag{4.3.3}$$

(see (4.5.16) for a full explanation in a general context), where

L_1 = expected number of codewords linked to the received sequence when a code with $(2^{nR^*}-1)$ independent codewords whose n components are generated independently according to a zero-mean Gaussian r.v. with variance P' is used over an AWGN cahnnel with noise variance N.

L_2 = expected number of codewords linked to the received sequence when a code with $(2^{nR^*}-1)^2$ independent codewords whose n components are independent zero-mean Gaussian r.v. with variance 2P' is used over the same channel.

From Shannon [29] we know that for sufficiently large n, $\forall\ \varepsilon > 0$,

$$L_1 \leq (2^{nR^*}-1)\, 2^{-n\left[\frac{1}{2}\log\left(1+\frac{P'}{N}\right)-\varepsilon\right]} \tag{4.3.4}$$

$$L_2 \leq (2^{nR^*}-1)^2\, 2^{-n\left[\frac{1}{2}\log\left(1+\frac{2P'}{N}\right)-\varepsilon\right]} \tag{4.3.5}$$

where we have used the union bound in (4.3.4) and (4.3.5). So, $\forall\ \varepsilon > 0$,

$$2L_1 + L_2 < 2^{nR^*}\left(2\cdot 2^{-\frac{n}{2}\log\left(1+\frac{P'}{N}\right)} + 2^{nR^*}\cdot 2^{-\frac{n}{2}\log\left(1+\frac{2P'}{N}\right)}\right) 2^{n\varepsilon} \tag{4.3.6}$$

$$= \left(2 + 2^{n\left[\log\left(1+\frac{P'}{N}\right)-\frac{1}{2}\log\left(1+\frac{2P'}{N}\right)\right]}\right)\ 2^{n\varepsilon} \tag{4.3.7}$$

But,

$$\log\left(1+\frac{P'}{N}\right) > \frac{1}{2}\log\left(1+\frac{2P'}{N}\right) \text{ if } \frac{P'}{N} > 0\ . \tag{4.3.8}$$

Therefore for n sufficiently large and $\varepsilon' > \varepsilon$,

$$2L_1 + L_2 \leq 2^{n\left[\log\left(1+\frac{P'}{N}\right)-\frac{1}{2}\log\left(1+\frac{2P'}{N}\right)+\varepsilon'\right]} \triangleq K. \tag{4.3.9}$$

Using Markov's inequality, we obtain

$$P_b \overset{\Delta}{=} \Pr\left\{|S_{\underline{y}}| > K2^{n\varepsilon_1}\right\} \leq 2^{-n\varepsilon_1}\ ,\ \varepsilon_1 > 0$$
$$< \varepsilon/5,\ \forall\ \varepsilon > 0 \text{ as } n \to \infty\ . \tag{4.3.10}$$

Note by inspection of (4.3.9) that in stage 1 the uncertainty of the receiver is reduced by $\frac{n}{2}\log\left(1+\frac{2P'}{N}\right)$ bits, precisely that which could be obtained (without feedback) if 1 and 2 were actually trying to communicate with Y rather than with each other.

$$\text{Let } P_F = \Pr\left\{\| \underline{x}_1(1) \|^2 > nP \text{ or } \| \underline{x}_2(1) \|^2 > nP\right\} \qquad (4.3.11)$$

where $$\| \underline{x}_i(1) \|^2 = \sum_{j=1}^{n} x_{ij}^2(1) \ , \ i = 1, 2. \qquad (4.3.12)$$

Now, $\frac{1}{n} \sum_{j=1}^{n} x_{ij}^2(1)$ is the arithmetic average of n independent identically distributed random variables with expected value $E\left(x_{ij}^2(1)\right) = P' < P$. By the law of large numbers, we know that $\Pr\left\{\| \underline{x}_i(1) \|^2 > nP, \ i = 1, 2\right\}$ can be made arbitrarily small. By the union bound, we can let $P_F < \varepsilon/5$.

Define E_1 as the event that stage 1 is successful, i.e.,

(1) $\| \underline{x}_1(1) \|^2 \leq nP$ and $\| \underline{x}_2(1) \|^2 \leq nP$ so that the codes satisfy the power constraints.

(2) $\underline{x}_1$ and $\underline{x}_2$ are correctly decoded at transmitters 2 and 1 respectively.

(3) the correct codeword $\underline{x}(1)$ is linked to the received sequence $\underline{y}$.

(4) $|S_{\underline{y}}| < K2^{n\varepsilon_1}$.

Let E_1^c denote the complement of this event. Then, by the union bound,

$$\overline{\Pr}\{E_1^c\} \leq P_{e_{1,2}} + P_{e_{1,1}} + (1-P_c) + P_b + P_F < \varepsilon \qquad (4.3.13)$$

where $\overline{\Pr}\{\cdot\}$ denotes expectation over the choice of codebooks and possible input messages.

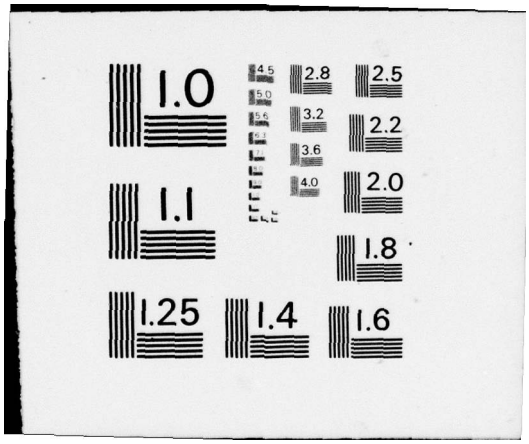
Therefore, there exists at least one code which satisfied the power constraints and has an average probability of failure in stage 1 less than ε. Since we can choose η to be arbitrarily small, the limiting value of R* is $\frac{1}{2} \log (1 + \frac{P}{N})$.

Assuming the first stage is successful, in stage 2 we have to send at most $n[\log (1 + \frac{P}{N}) - \frac{1}{2} \log (1 + \frac{2P}{N}) + \varepsilon]$ bits to the receiver in

AD-A032 751 STANFORD UNIV CALIF STANFORD ELECTRONICS LABS F/G 17/2
MULTI-USER AND WIRETAP CHANNELS INCLUDING FEEDBACK.(U)
JUL 76 S K LEUNG-YAN-CHEONG F44620-73-C-0065
UNCLASSIFIED TR-6603-2 AFOSR-TR-76-1197 NL

2 OF 2
ADA032751

END
DATE FILMED
1 - 77


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6

order to specify completely the correct codeword. But in stage 2, the two transmitters can cooperate totally since they both know the correct codeword. They both send the same signal. Thus, the signals add coherently at the receiver for stage 2. Because of the additive nature of the channel, total cooperation between the two senders allows reliable transmission (i.e. with a probability of error $P_{e_2} < \varepsilon$) up to a rate of $\frac{1}{2} \log (1 + \frac{4P}{N})$ bits/transmission i.e., the effective power is now $(\sqrt{P} + \sqrt{P})^2 = 4P$ instead of $P + P = 2P$.

We define the probability of failure P_f as the probability that at the end of stage 2, the receiver does not correctly estimate the messages sent from the 2 transmitters. Thus $P_f \leq Pr\{E_1^c\} + P_{e_2} < 2\varepsilon$, which means the proposed scheme allows reliable transmission.

We now calculate the effective achievable rate. The number of transmissions required for stage 2 is

$$\frac{n \left[\log (1 + \frac{P}{N}) - \frac{1}{2} \log (1 + \frac{2P}{N}) + \varepsilon\right]}{\frac{1}{2} \log (1 + \frac{4P}{N})} \tag{4.3.14}$$

We recall that stage 1 requires n transmissions, and that the total amount of information conveyed from the two senders to the receiver in both stages is $n \log (1 + \frac{P}{N})$ bits. So the overall effective rate $R_1 + R_2$ is (as $\varepsilon \to 0$)

$$\frac{n \log (1 + \gamma)}{n + n \left[\log (1 + \gamma) - \frac{1}{2} \log(1 + 2\gamma)\right]/\left[\frac{1}{2} \log (1 + 4\gamma)\right]} \tag{4.3.15}$$

$$= \frac{\log (1 + \gamma) \log (1 + 4\gamma)}{\log (1 + 4\gamma) + 2 \log (1 + \gamma) - \log (1 + 2\gamma)} \quad \text{bits/transmission} \tag{4.3.16}$$

where $\gamma \triangleq P/N$

Figure 4.4 shows the point, * , which can be achieved by the proposed scheme for $\gamma = 5$.

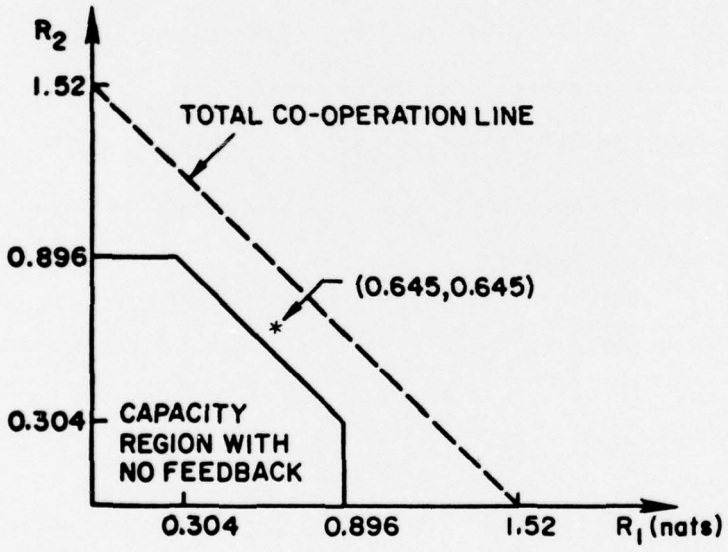


Figure 4.4 - CAPACITY REGION OF AWGN MULTIPLE-ACCESS CHANNEL WITH γ=5. RATES ARE IN NATS/TRANSMISSION.

In the asymmetric case, suppose $P_1 > P_2$. We would like the two transmitters to learn each other's message after an equal number of transmissions so that they are ready to cooperate at the same time. So we choose to transmit mR_1 and mR_2 bits to the receiver from transmitters

1 and 2 respectively where $R_1 = \frac{1}{2} \log (1 + \frac{P_1}{N})$ and $R_2 = \frac{1}{2} \log (1 + \frac{P_2}{N})$ and m is some large number. It is not difficult to see that this scheme will yield a point outside the capacity region with no feedback.

4.4 JOINTLY TYPICAL SEQUENCES

In this section we recall some basic results concerning typical sequences which will be used to find out when feedback can increase the capacity region of discrete memoryless multiple-access channels.

Let $\{X^{(1)}, X^{(2)}, \ldots, X^{(k)}\}$ denote a finite collection of discrete random variables with some fixed joint distribution $p(x^{(1)}, x^{(2)}, \ldots, x^{(k)})$. Let S denote an ordered subset of these random variables and consider n independent copies of S. Thus,

$$\Pr\{\underline{S} = \underline{s}\} = \prod_{i=1}^{n} \Pr\{S_i = s_i\} \tag{4.4.1}$$

For example, if $S = \left(X^{(j)}, X^{(k)}\right)$, then

$$\Pr\{\underline{S} = \underline{s}\} = \Pr\left\{\left(\underline{X}^{(j)}, \underline{X}^{(k)}\right) = \left(\underline{x}^{(j)}, \underline{x}^{(k)}\right)\right\} \tag{4.4.2}$$

$$= \prod_{i=1}^{n} p\left(x_i^{(j)}, x_i^{(k)}\right)$$

Definition: The set A_ε of jointly ε-typical n-sequences $\left(\underline{x}^{(1)}, \underline{x}^{(2)}, \ldots, \underline{x}^{(k)}\right)$ is defined by

$$A_\varepsilon\left(X^{(1)},X^{(2)},\ldots,X^{(k)}\right) = \Big\{\left(\underline{x}^{(1)},\underline{x}^{(2)},\ldots,\underline{x}^{(k)}\right) \in \left(\mathcal{X}^{(1)}\right)^n \times \left(\mathcal{X}^{(2)}\right)^n \times \ldots \times \left(\mathcal{X}^{(k)}\right)^n : \left| -\frac{1}{n}\log p(\underline{s}) - H(S)\right| \leq \varepsilon,\ \forall\ S \subseteq \left\{X^{(1)},X^{(2)},\ldots X^{(k)}\right\}\Big\} \quad (4.4.3)$$

where $\underline{s}$ denotes the ordered set of sequences in $\left\{\underline{x}^{(1)},\ldots,\underline{x}^{(k)}\right\}$ corresponding to S. Let $A_\varepsilon(S)$ denote the restriction of A_ε to the coordinates corresponding to S. Thus, for example, for $S = (X^{(1)},X^{(3)})$,

$$A_\varepsilon\left(X^{(1)},X^{(3)}\right) = \Big\{\left(\underline{x}^{(1)},\underline{x}^{(3)}\right) : \left| -\frac{1}{n}\log p\left(\underline{x}^{(1)},\underline{x}^{(3)}\right) - H\left(X^{(1)},X^{(3)}\right)\right| < \varepsilon,$$

$$\left| -\frac{1}{n}\log p\left(\underline{x}^{(1)}\right) - H\left(X^{(1)}\right)\right| < \varepsilon,$$

$$\left| -\frac{1}{n}\log p\left(\underline{x}^{(3)}\right) - H\left(X^{(3)}\right)\right| < \varepsilon\Big\} \quad (4.4.4)$$

We now recall three basic lemmas. For a proof of these lemmas, see Forney [30] and Cover [10].

Lemma 4.1: For any $\varepsilon > 0$, there exists an integer n such that $A_\varepsilon(S)$ satisfies, for all $S \subseteq \{X^{(1)},\ldots,X^{(k)}\}$,

$$\text{(i)}\quad \Pr\{A_\varepsilon(S)\} \geq 1 - \varepsilon,$$

$$\text{(ii)}\quad \underline{s} \in A_\varepsilon(S) \Rightarrow \left| -\frac{1}{n}\log p(\underline{s}) - H(S)\right| < \varepsilon \quad (4.4.5)$$

$$\text{(iii)}\quad (1-\varepsilon)2^{n(H(S)-\varepsilon)} \leq |A_\varepsilon(S)| \leq 2^{n(H(S)+\varepsilon)}$$

Lemma 4.2: Let the discrete random variables X,Y have joint distribution $p(x,y)$. Let X' and Y' be independent but with the same marginals

$$p(x) = \sum_{y} p(x,y)$$

$$p(y) = \sum_{x} p(x,y)$$

as X and Y.

Let $(\underline{X},\underline{Y}) \sim \prod_{i=1}^{n} p(x_i,y_i)$ and $(\underline{X}',\underline{Y}') \sim \prod_{i=1}^{n} p(x_i)p(y_i)$ where X_i and Y_i, $1 \leq i \leq n$ are independent and identically distributed as X and Y respectively. Then

$$\Pr\{(\underline{X}',\underline{Y}') \in A_\varepsilon (X,Y)\} \leq 2^{-n[I(X;Y) - \varepsilon]} \qquad (4.4.6)$$

Lemma 4.3: Let the discrete random variables X,Y,Z have joint distribution $p(x,y,z)$. Let X',Y' be conditionally independent given Z, with the marginals

$$p(x|z) = \sum_{y} \frac{p(x,y,z)}{p(z)}$$

$$p(y|z) = \sum_{x} \frac{p(x,y,z)}{p(z)} \qquad (4.4.7)$$

Let $(\underline{X},\underline{Y},\underline{Z}) \sim \prod_{i=1}^{n} p(x_i,y_i,z_i)$ and

$$(\underline{X}',\underline{Y}',\underline{Z}) \sim \prod_{i=1}^{n} p(x_i|z_i)p(y_i|z_i)p(z_i) \ .$$

Then $$\Pr\{(\underline{X}',\underline{Y}',\underline{Z}) \in A_\varepsilon\ (X,Y,Z)\} \leq 2^{-n[I(X;Y|Z) - \varepsilon]} \qquad (4.4.8)$$

4.5 THE DISCRETE MEMORYLESS MULTIPLE-ACCESS CHANNEL

In this section, we shall find conditions under which the proposed scheme will increase the capacity region of discrete memoryless multiple-access channels. In particular we shall prove the following.

Theorem 4.1

Let Q_1 and Q_2 denote probability distributions on X_1 and X_2 respectively. Suppose that $Q^* = (Q_1^*,Q_2^*)$ achieves the maximum of $I(X_1,X_2;Y)$ over all product distributions $Q_1(x_1)Q_2(x_2)$. Then the proposed feedback scheme allows reliable transmission at an overall effective rate of

$$R_1 + R_2 = \frac{AB}{A+B-C} \qquad (4.5.1)$$

where $$A \triangleq I_{Q^*}(X_1;Y|X_2) + I_{Q^*}(X_2;Y|X_1) \qquad (4.5.2)$$

$$B \triangleq \max_{p(x_1,x_2)} I(X_1,X_2;Y) \qquad (4.5.3)$$

and $C \stackrel{\Delta}{=} I_{Q^*}(X_1,X_2;Y)$ is the maximum non-feedback sum rate. (4.5.4)

Remark: The maximum in the expression for B is taken over all joint distributions of X_1 and X_2.

Corollary: Sufficient conditions under which feedback will increase the capacity region are $A,B > C$, i.e.,

$$\text{(i)} \quad I_{Q^*}(X_1;Y|X_2) + I_{Q^*}(X_2;Y|X_1) > I_{Q^*}(X_1,X_2;Y) \tag{4.5.5}$$

$$\text{(ii)} \quad \max_{p(x_1,x_2)} I(X_1,X_2;Y) > I_{Q^*}(X_1,X_2;Y) \tag{4.5.6}$$

Remark: Notice that (ii) is a necessary condition for feedback to increase the capacity region.

Proof of Corollary: We want to show that if $A > C$ and $B > C$, then

$$\frac{AB}{A+B-C} > C \tag{4.5.7}$$

Let $A = C + \alpha$ and $B = C + \beta$ where $\alpha,\beta > 0$. (4.5.8)

Then

$$C^2 + \alpha C + C\beta + \alpha\beta > C^2 + \alpha C + \beta C \tag{4.5.9}$$

i.e. $$\frac{(C + \alpha)(C + \beta)}{C + \alpha + \beta} > C \tag{4.5.10}$$

i.e. $$\frac{AB}{A+B-C} > C \qquad \square$$

We now proceed to prove theorem 4.1.

Consider a stage 1 randomly generated code of blocklength n and rates R_{12}, R_{21} obtained as follows. Each codeword $\underline{x}_i$, $i = 1,2$ is an n-sequence of independent outcomes of a random variable distributed according to Q_i^*. We generate $2^{nR_{12}}$ independent $\underline{x}_1$'s and $2^{nR_{21}}$ independent $\underline{x}_2$'s. Let these be indexed as $\underline{x}_1(k)$, $k \in \left[1,2^{nR_{12}}\right]$ and $\underline{x}_2(\ell)$, $\ell \in \left[1,2^{nR_{21}}\right]$.

Let K,L be independent random variables drawn according to uniform distributions on $\left[1,2^{nR_{12}}\right]$ and $\left[1,2^{nR_{21}}\right]$ respectively. Let the code be chosen randomly from the above ensemble. As in section 4.3, we first proceed to upper bound the average probability $\overline{Pr}\{E_1^c\}$ that stage 1 is unsuccessful. By the symmetry induced by the random coding, we see that each transmitted message (k,ℓ) yields the same probability of error. So hence forth we shall assume that the actual transmitted message is $(1,1)$.

The decoding rule for estimating the message of the first transmitter at the second transmitter (at the end of stage 1) is as follows. If $\underline{y}$ is received, declare $\hat{k} = k$ was sent if and only if there is only one $k \in \left[1,2^{nR_{12}}\right]$ such that $(\underline{x}_1(k),\underline{x}_2(1),\underline{y})$ are jointly typical. Using lemmas 4.1 and 4.3, it can be shown (for details see [10]) that k can be decoded with arbitrarily small probability of error, say, $P_{e_{1,2}} < \varepsilon/4$ if

$$R_{12} < I_{Q^*}(X_1;Y|X_2) \tag{4.5.11}$$

and n is sufficiently large. Similarly ℓ can be estimated at the first transmitter with arbitrarily small probability of error, say , $P_{e_{1,1}} < \varepsilon/4$ if

$$R_{21} < I_{Q^*}(X_2;Y|X_1) \tag{4.5.12}$$

We now consider the set $S_{\underline{y}}$ of codewords which, at the end of stage 1, are jointly typical with $\underline{y}$. From lemma 4.1, we know that $(\underline{x}_1(1),\underline{x}_2(1))$ will be jointly typical with $\underline{y}$ with high probability, say,

$$P_c > 1 - \varepsilon/4 . \tag{4.5.13}$$

Let $$\psi_{k,\ell}(\underline{y}) = \begin{cases} 1 , & (\underline{x}_1(k),\underline{x}_2(\ell),\underline{y}) \text{ are typical} \\ 0 , & \text{otherwise} \end{cases} \tag{4.5.14}$$

Then $$|S_{\underline{y}}| = \sum_{k,\ell} \psi_{k,\ell}(\underline{y}) \tag{4.5.15}$$

$$E|S_{\underline{y}}| = \sum_{k=1,\ell=1} E\psi_{k,\ell}(\underline{y}) + \sum_{k\neq 1,\ell=1} E\psi_{k,\ell}(\underline{y}) +$$

$$\sum_{k=1,\ell\neq 1} E\psi_{k,\ell}(\underline{y}) + \sum_{k\neq 1,\ell\neq 1} E\psi_{k,\ell}(\underline{y}) \tag{4.5.16}$$

Using lemmas 4.2 and 4.3, it can be shown that

$$E\psi_{k,\ell}(\underline{y}) \leq 2^{-n\left[I_{Q^*}(X_1,X_2;Y) - \varepsilon \right]} , \quad k\neq 1, \ \ell\neq 1 \tag{4.5.17}$$

$$E\psi_{1,\ell}(\underline{y}) \leq 2^{-n\left[I_{Q^*}(X_2;Y|X_1) - \varepsilon\right]}, \quad k=1,\ \ell\neq 1 \tag{4.5.18}$$

$$E\psi_{k,1}(\underline{y}) \leq 2^{-n\left[I_{Q^*}(X_1;Y|X_2) - \varepsilon\right]}, \quad k\neq 1,\ \ell=1 \tag{4.5.19}$$

Therefore,

$$\begin{aligned} E|S_{\underline{y}}| \leq 1 &+ \left(2^{nR_{12}}-1\right)\left(2^{nR_{21}}-1\right)\ 2^{-n\left[I_{Q^*}(X_1,X_2;Y) - \varepsilon\right]} \\ &+ \left(2^{nR_{12}}-1\right)\ 2^{-n\left[I_{Q^*}(X_1;Y|X_2) - \varepsilon\right]} \\ &+ \left(2^{nR_{21}}-1\right)\ 2^{-n\left[I_{Q^*}(X_2;Y|X_1) - \varepsilon\right]} \end{aligned} \tag{4.5.20}$$

Taking the limit in (4.5.11) and (4.5.12) we can set $R_{12} = I_{Q^*}(X_1;Y|X_2)$ and $R_{21} = I_{Q^*}(X_2;Y|X_1)$. Then (4.5.20) becomes

$$E|S_{\underline{y}}| < 1 + 2\cdot 2^{n\varepsilon} + 2^{n\left[I_{Q^*}(X_1;Y|X_2) + I_{Q^*}(X_2;Y|X_1) - I_{Q^*}(X_1,X_2;Y) + \varepsilon\right]} \tag{4.5.21}$$

$$< 2^{n(D+\varepsilon_1)}, \tag{4.5.22}$$

where $$D = I_{Q^*}(X_1;Y|X_2) + I_{Q^*}(X_2;Y|X_1) - I_{Q^*}(X_1,X_2;Y) \tag{4.5.23}$$

Using Markov's inequality we obtain

$$P_b \triangleq \Pr\left\{|S_{\underline{y}}| > 2^{n\varepsilon_2}\ 2^{n(D+\varepsilon_1)}\right\} < 2^{-n\varepsilon_2}$$

$$< \varepsilon/4 \quad \text{say} \tag{4.5.24}$$

From (4.3.13)

$$\overline{Pr}\left\{E_1^c\right\} \leq P_{e_{1,2}} + P_{e_{1,1}} + (1 - P_c) + P_b \qquad (4.5.25)$$

$$< \varepsilon \qquad (4.5.26)$$

Since $\overline{Pr}\left\{E_1^c\right\} < \varepsilon$, there must exist at least one code with an average probability of failure (taken over K,L) in stage 1 less than ε.

Assuming the first stage is successful, in stage 2 we have to send at most $n(D + \varepsilon_1)$ bits to the receiver in order to completely specify the correct code word. In stage 2, total cooperation between the two transmitters allows transmission up to a rate of $\max_{p(x_1,x_2)} I(X_1,X_2;Y)$ with arbitrarily small probability of error, say $P_{e_2} < \varepsilon$. Thus the probability of failure $P_f \leq Pr\left\{E_1^c\right\} + P_{e_2} < 2\varepsilon$, which means that the scheme allows reliable transmission. A straight forward calculation shows that the overall effective sum rate using this scheme is

$$R_1 + R_2 = \frac{\left[I_{Q^*}(X_1;Y|X_2) + I_{Q^*}(X_2;Y|X_1) \right] \max_{p(x_1,x_2)} I(X_1,X_2;Y)}{\max_{p(x_1,x_2)} I(X_1,X_2;Y) + I_{Q^*}(X_1;Y|X_2) + I_{Q^*}(X_2;Y|X_1) - I_{Q^*}(X_1,X_2;Y)} \qquad (4.5.27)$$

This completes the proof of theorem 4.1.

4.6 CONCLUDING REMARKS

The capacity region of multiple-access channels with feedback can generally be increased by the scheme of transmitting first at high rates until both transmitters know each other's messages, then cooperatively at a lower rate to resolve the remaining receiver ambiguity. An open problem is to determine the full capacity region with feedback and conditions, if any, under which the above scheme is optimal. Finally we might mention that feedback can increase the capacity region of interference channels which are channels with an equal number of senders and receivers, and in which each sender wishes to communicate with a corresponding receiver.

CHAPTER 5

CONCLUSIONS

In chapter 2, we introduced the additive white Gaussian noise wiretap channel and explicitly determined the set $\mathcal{R}^*$ of all achievable rate-equivocation pairs. It turns out that the secrecy capacity C_s is the difference between the capacities of the main and wiretapper's channels, and increases monotonically as the input power constraint is relaxed. The quantity C_s almost completely specifies $\mathcal{R}^*$. Some useful characterizations of a special class of wiretap channels are mentioned in section 2.4.

Chapter 3 dealt with the wiretap channel with feedback. It is shown that with the introduction of feedback, even when the main channel is inferior to the wiretapper's channel, it is still possible to send reliably at a positive rate to the legitimate receiver while at the same time keeping the wiretapper in total ignorance. The binary erasure wiretap channel with feedback is studied in detail and inner and outer bounds on the achievable (R,d) region are given.

In Chapter 4 we analyzed a scheme for enlarging the capacity region of multiple-access channels using feedback. It is shown that the capacity region can generally be increased by the scheme of transmitting first at high rates until both receivers know each other's messages, then cooperatively at a lower rate to resolve the remaining receiver ambiguity.

Among the problems which deserve further study, we may mention the

following.

1. The formulation of a good coding scheme for use on wiretap channels with feedback.
2. The proof of a tight outerbound on the achievable (R,d) region for wiretap channels with feedback.
3. The determination of the capacity region of multiple-access channels with feedback.
4. The effect of noisy feedback in the problems examined in the preceeding chapters.
5. The extension of the notions of privacy, security and secrecy to networks involving several senders and receivers. This would lead to a generalization of the wiretap channel.

APPENDIX I

In this appendix, we show that for the example in which the main channel and the wiretap channel are binary symmetric channels with crossover probabilities 0 and ε respectively, $\Gamma(R)$ as defined in (2.1.5) is equal to $h(\varepsilon)$. See Wyner [19].

Proof:

$$I(X;Y|Z) = H(X|Z) - H(X|Y,Z) \tag{A.1.1}$$

$$= H(X|Z) - H(X|Y) \tag{A.1.2}$$

(A.1.2) holds because X and Z are independent conditioned on Y. Since the main channel is noiseless, we have that $H(X|Y) = 0$. So

$$I(X;Y|Z) = H(X) - H(Z) + H(Z|X) \tag{A.1.3}$$

$$H(Z|X) = \sum_{x,z\in\{0,1\}} p(x,z) \log \frac{1}{p(z|x)} \tag{A.1.4}$$

$$= \varepsilon \log \frac{1}{\varepsilon} + (1-\varepsilon) \log \frac{1}{(1-\varepsilon)} \tag{A.1.5}$$

$$\stackrel{\Delta}{=} h(\varepsilon) \tag{A.1.6}$$

Therefore, in order to maximize $I(X;Y|Z)$, we need to maximize $H(X) - H(Z)$.

We now recall a result which will be useful in lower-bounding $H(Z) - H(X)$.

Lemma A.1.1

Let X and Z denote the input and output respectively of a binary symmetric channel. Then

$$H(Z) \geq H(X) \tag{A.1.7}$$

Proof: Follows from Mrs. Gerber's Lemma [22].

At $q_0 = \frac{1}{2}$, $H(Z) = H(X)$. Therefore the maximum value of $I(X;Y|Z)$ is $h(\varepsilon)$ and is attained when $Pr\{X=0\} = Pr\{X=1\} = \frac{1}{2}$. But this input distribution also achieves the capacity of the main channel. Thus,

$$\Gamma(R) = h(\varepsilon), \quad 0 \leq R \leq 1 . \tag{A.1.8}$$

APPENDIX II

We give examples of two frequently encountered constant $\Gamma(R)$ wiretap channels.

Example 1

Referring to figure 2.1, let the main channel be a noiseless binary channel and the wiretap channel be a binary erasure channel (BEC) with erasure rate ε .

Following (A.1.3) we can write

$$I(X;Y|Z) = H(X) - H(Z) + H(Z|X) \qquad (A.2.1)$$

Let $Pr\{X=0\} = q_0$ and $Pr\{X=1\} = 1-q_0$. A straightforward calculation yields

$$H(Z|X) = h(\varepsilon) \qquad (A.2.2)$$

Therefore, to maximize $I(X;Y|Z)$ it is sufficient to maximize $H(X) - H(Z)$.

$$H(X) - H(Z) = -q_0 \log q_0 - (1-q_0) \log (1-q_0) + q_0 (1-\varepsilon) \log q_0 (1-\varepsilon) + \varepsilon \log \varepsilon + (1-q_0) (1-\varepsilon) \log (1-q_0) (1-\varepsilon) \qquad (A.2.3)$$

Differentiating (A.2.3) with respect to q_0 and carrying out the algebra yields

$$\frac{d}{dq_0} (H(X) - H(Z)) = \varepsilon \log \left(\frac{1-q_0}{q_0} \right) . \qquad (A.2.4)$$

Setting (A.2.4) equal to zero, we find that $q_0 = \frac{1}{2}$ corresponds to a stationary point. Examination of the second derivative shows that the point $q_0 = \frac{1}{2}$ is a maximum. Thus,

$$I(X;Y|Z) = 1 - [\, 1-\varepsilon + h(\varepsilon) \,] + h(\varepsilon)$$

$$= \varepsilon$$

Since $q_0 = \frac{1}{2}$ is also the capacity achieving distribution of the main channel, we conclude that

$$\Gamma(R) = \varepsilon \ , \quad 0 \leq R \leq C_M = 1 \ . \qquad \text{(A.2.5)}$$

Figure A.1 shows the complete achievable (R,d) region for the above example.

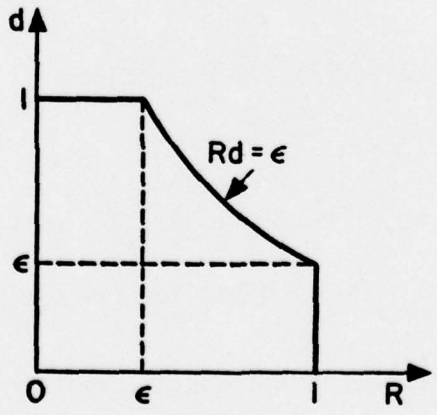


Figure A.1 - (R,d) REGION FOR BE WIRETAP CHANNEL

Example 2 (see figure 2.1)

We consider the case in which the main and wiretap channels are binary symmetric channels (BSC) with crossover probabilities ε_1 and ε_2 respectively.

From (A.1.2) we have

$$I(X;Y|Z) = H(X|Z) - H(X|Y) \tag{A.2.6}$$

$$= [H(X) + H(Z|X) - H(Z)] - [H(X) + H(Y|X) - H(Y)] \tag{A.2.7}$$

$$= H(Z|X) - H(Y|X) - [H(Z) - H(Y)] \tag{A 2.8}$$

Definition A.1: For $0 \leq a, b \leq 1$, define

$$a * b = a(1-b) + b(1-a) . \tag{A.2.9}$$

Then it can be shown that

$$H(Y|X) = h(\varepsilon_1) \tag{A.2.10a}$$

and

$$H(Z|X) = h(\varepsilon_1 * \varepsilon_2) . \tag{A.2.10b}$$

Therefore, the problem of maximizing $I(X;Y|Z)$ is equivalent to that of minimizing $H(Z) - H(Y)$. From lemma A.1.1 we know that

$$H(Z) \geq H(Y) . \tag{A.2.11}$$

Also the input distribution $Pr\{X=0\} = Pr\{X=1\} = \frac{1}{2}$ achieves $H(Z) = H(Y)$. But this distribution achieves the capacity of the main channel as well.

This proves that

$$\Gamma(R) = h(\varepsilon_1 * \varepsilon_2) - h(\varepsilon_1) \ , \quad 0 \leq R \leq (1-h(\varepsilon_1)) \qquad (A.2.12)$$

REFERENCES

1. C. E. Shannon, "A Mathematical Theory of Communication," Bell System Technical Journal, Vol. 27, pp. 379-423 and 623-656, July and October 1948.

2. D. Slepian (editor), Key Papers in the Development of Information Theory, IEEE Press, New York, 1974.

3. R. G. Gallager, Information Theory and Reliable Communication, Wiley, New York 1968.

4. T. M. Cover, "Broadcast Channels," IEEE Trans. on Info. Theory, Vol. IT-18, pp. 2-14, January 1972.

5. P. P. Bergmans, "Random Coding Theorem for Broadcast Channels with Degraded Components," IEEE Trans. on Info. Theory, Vol. IT-19, pp. 197-207, March 1973.

6. A. D. Wyner, "A Theorem on the Entropy of Certain Binary Sequences and Applications: Part II," IEEE Trans. on Info. Theory, Vol. IT-19, pp. 772-777, November 1973.

7. R. G. Gallager, "Capacity and Coding for Degraded Broadcast Channels," Problemy Peredachi Informatsii, Vol. 10, pp. 3-14, July-September 1974.

8. P. P. Bergmans and T. M. Cover, "Cooperative Broadcasting," IEEE Trans. on Info. Theory, Vol. IT-20, pp. 317-324, May 1974.

9. P. P. Bergmans, "A Simple Converse for Broadcast Channels with Additive White Gaussian Noise," IEEE Trans. on Info. Theory, Vol. IT-20, pp. 279-280, March 1974.

10. T. M. Cover, "An Achievable Rate Region for the Broadcast Channel," IEEE Trans. on Info. Theory, Vol. IT-21, pp. 399-404, July 1975.

11. E. C. van der Meulen, "Random Coding Theorems for the General Discrete Memoryless Broadcast Channel," IEEE Trans. on Info. Theory, Vol. IT-21, pp. 180-190, March 1975.

12. T. M. Cover, Personal Communication.

13. D. Slepian and J. K. Wolf, "A Coding Theorem for Multiple-Access Channels with Correlated Sources," The Bell System Technical Journal, Vol. 52, pp. 1037-1076, September 1973.

14. R. Ahlswede, "Multi-way Communication Channels," Proc. of 2nd International Symposium on Information Transmission, Tsahkadsor, Armenia, USSR, 1971, Hungarian Press.

15. H. Liao, "Multiple-Access Channels," Ph.D. Dissertation, Dept. of Elec. Eng., University of Hawaii, Honolulu, 1972.

16. A. D. Wyner, "Recent Results in the Shannon Theory," IEEE Trans. on Info. Theory, Vol. IT-20, pp. 2-10, January 1974.

17. T. M. Cover, "Some Advances in Broadcast Channels," chapter in Advances in Communication Systems, Vol. 4, Theory and Applications, Ed. by A. Viterbi, Ac. Press, S.F., 1975.

18. C. E. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, Vol. 28, pp. 656-715, 1949.

19. A. D. Wyner, "The Wire-tap Channel," Bell System Technical Journal, Vol. 54, pp. 1355-1387, October 1975.

20. M. E. Hellman and A. B. Carleial, "A Note on Wyner's Wiretap Channel," to appear IEEE Trans. on Info. Theory.

21. R. Ash, Information Theory, Interscience, New York, 1965.

22. A. D. Wyner and J. Ziv, "A Theorem on the Entropy of Certain Binary Sequences and Applications: Part I," IEEE Trans. on Info. Theory, Vol. IT-19, pp. 769-772, November 1973.

23. N. M. Blachman, "The Convolution Inequality for Entropy Powers," IEEE Trans. on Info. Theory, Vol. IT-11, pp. 267-271, April 1965.

24. L. Cooper and D. Steinberg, Introduction to Methods of Optimization, Saunders, Philadelphia, 1970.

25. C. E. Shannon, "The zero-error capacity of a noisy channel," IRE Trans. on Info. Theory, Vol. IT-2, pp. 8-19, September 1956.

26. J. P. M. Schalkwijk and T. Kailath, "A Coding Scheme for Additive Noise Channels with Feedback," IEEE Trans. on Info. Theory, IT-12, pp. 172-182 and 183-189, April 1966.

27. N. T. Gaarder and J. K. Wolf, "The Capacity Region of a Multiple-Access Discrete Memoryless Channel Can Increase with Feedback," IEEE Trans. on Info. Theory, IT-21, pp. 100-102, January 1975.

28. T. M. Cover and S. K. Leung-Yan-Cheong, "A Scheme for Enlarging the Capacity Region of Multiple-Access Channels using Feedback," Technical Report No. 17, Department of Statistics, Stanford University, Stanford, California 94305, March 1976.

29. C. E. Shannon, "Communication in the Presence of Noise," Proc. IRE, Vol. 37, pp. 10-21, January 1949.

30. G. D. Forney, "Information Theory," course notes for EE-376, Stanford University Electrical Engineering Dept., Stanford, California 94305, 1972.

31. M. E. Hellman, "An Extension of the Shannon Theory Approach to Cryptography," to appear IEEE Trans. on Info. Theory.